(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号
特表2001－521261
（P2001－521261A）
(43)公表日　平成13年11月６日(2001.11.6)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード(参考)
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ	５Ｃ０５３
			Ｄ	５Ｄ０４４
Ｈ０４Ｎ　5/91		Ｈ０４Ｎ　5/91	Ｐ	
5/92		5/92	Ｈ	

審査請求　未請求　予備審査請求　有　（全 47 頁）

(21)出願番号　特願2000－518385(P2000－518385)
(86)(22)出願日　平成10年10月19日(1998.10.19)
(85)翻訳文提出日　平成12年４月24日(2000.4.24)
(86)国際出願番号　ＰＣＴ／ＵＳ９８／２２１２６
(87)国際公開番号　ＷＯ９９／２２３７２
(87)国際公開日　平成11年５月６日(1999.5.6)
(31)優先権主張番号　０８／９５７，０５１
(32)優先日　平成９年10月24日(1997.10.24)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　ソニー　エレクトロニクス　インク
アメリカ合衆国　ニュージャージー州　07656　パークリッジ　ソニー　ドライブ　1
(72)発明者　小室　輝芳
日本国神奈川県川崎市宮前区鷺沼３－11－130－101
(72)発明者　大澤　義知
日本国神奈川県横浜市青葉区美しが丘１－10－２－502
(74)代理人　弁理士　小池　晃　（外２名）

最終頁に続く

(54)【発明の名称】　伝送システム及び伝送方法

(57)【要約】
暗号モード識別子（ＥＭＩ）を用いて情報を伝送する伝送方法及び伝送システムに関する。本発明は、（例えば、音声／画像作品を示す）データが、ソース装置からシンク装置（受信局）に伝送される際に用いられる複数の保護通信モードを提供する。第１の保護モードであるＥＭＩモードＡでは、伝送される情報が、作品全体に渡ってコピーが許可されない。これは、最も高レベルのコピー禁止である。第２の保護モードであるＥＭＩモードＢでは、伝送される情報が、シンク装置によって一世代コピーのみを許可される。第３の保護モードでは、暗号化が行われず、自由なコピーが可能である。モードＡ及びモードＢのいずれの保護モードが選択されるかによって、ソース装置は伝送情報を暗号化する際に異なる暗号化処理を用いる。更に、モードＡ及びモードＢのいずれの保護モードが選択されるかによって、シンク装置は伝送情報を暗号解読する際に異なる暗号解読処理を用いる。本発明は、ソース装置と、パケットヘッダからコピー制御情報を抽出する能力を備えていないビットストリーム記録装置との間での伝送に特に有効である。各伝送

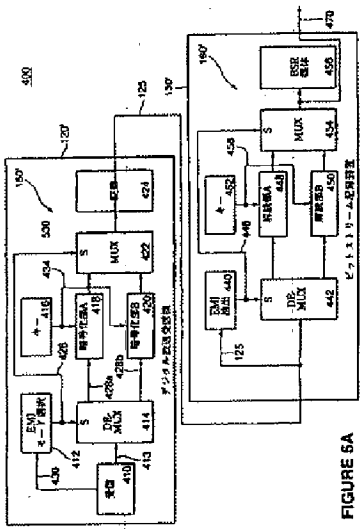

FIGURE 5A

【特許請求の範囲】

【請求項１】　情報を伝送する伝送システムにおいて、

暗号化モード識別子（ＥＭＩ）コードが第１のモードを示すときに、情報パケットのデータを暗号化する第１の暗号回路と、上記ＥＭＩコードが第２のモードを示すときに、上記情報パケットのデータを暗号化する第２の暗号回路とを有し、上記ＥＭＩコードをエンコードして上記情報パケットにして、上記情報パケットを通信インタフェースを介して伝送するソース装置と、

上記通信パケットから上記ＥＭＩコードを抽出する抽出回路と、上記ＥＭＩコードが上記第２のモードであることを示す上記抽出回路に反応して、上記情報パケットのデータを暗号解読する第２の暗号解読回路とを有し、上記通信インタフェースから上記情報パケットを受信するシンク装置とを備え、

上記第１のモードは、上記情報パケットが上記シンク装置によって再生されないことを示すコピー禁止モードであり、上記第２のモードは、上記情報パケットが上記シンク装置によって１回以上再生されないことを示す１回コピー許可モードであることを特徴とする伝送システム。

【請求項２】　上記シンク装置は、更に、上記ＥＭＩコードが上記第１のモードであることを示す上記抽出回路に反応して、上記情報パケットのデータを暗号解読する第１の暗号解読回路を備えることを特徴とする請求項１記載の伝送システム。

【請求項３】　上記第１の暗号回路と、上記第２の暗号回路と、第１の暗号解読回路と、第２の暗号解読回路は接続され、１個の等しい暗号キーを受信することを特徴とする請求項２記載の伝送システム。

【請求項４】　情報を伝送する伝送システムにおいて、

暗号化モード識別子（ＥＭＩ）コードが第１のモードを示すときに、第１のキーに基づいて情報パケットのデータを暗号化する共通の暗号回路を有し、上記ＥＭＩコードをエンコードして上記情報パケットにして、上記情報パケットを通信インタフェースを介して伝送するソース装置と、

上記通信パケットから上記ＥＭＩコードを抽出する抽出回路と、上記ＥＭＩコードが上記第２のモードであることを示す上記抽出回路に反応して、上記第２の

キーを用いて上記情報パケットのデータを暗号解読する共通の暗号解読回路とを有し、上記通信インタフェースから上記情報パケットを受信するシンク装置とを備え、

上記第１のモードは、上記情報パケットが上記シンク装置によって再生されないことを示すコピー禁止モードであり、上記第２のモードは、上記情報パケットが上記シング装置によって１回以上再生されないことを示す１回コピー許可モードであることを特徴とする伝送システム。

【請求項５】　上記シンク装置はビットストリーム記録装置であり、上記シンク装置は、更に、上記ＥＭＩコードが上記第２のモードであるときに上記情報パケットを記録する記録媒体を備え、上記記録媒体に記録された後、上記シンク装置によって、上記情報パケットの上記ＥＭＩコードが上記第２のモードに変換されることを特徴とする請求項１又は４記載の伝送システム。

【請求項６】　上記シンク装置の上記共通の暗号解読回路は、また、上記ＥＭＩコードが上記第１のモードであることを示す上記抽出回路に反応して、上記第１のキーを用いて上記情報パケットのデータを暗号解読するためのものであることを特徴とする請求項４記載の伝送システム。

【請求項７】　上記通信インタフェースは、ＩＥＥＥ１３９４通信規格に準拠したシリアル通信インタフェースであり、上記情報パケットはデジタルの情報パケットであることを特徴とする請求項２又は６記載の伝送システム。

【請求項８】　上記ソース装置は放送受信装置であり、更に、コピー制御情報（ＣＣＩ）を用いてエンコードされた情報パケットを受信し、コピー保護コードを抽出する受信回路を備え、上記シンク装置は、ＣＣＩ情報を用いてエンコードされた情報パケットを処理することができないことを特徴とする請求項２又は６記載の伝送システム。

【請求項９】　上記情報パケットは、１まとまりのデジタルの音声／画像プログラムを示すことを特徴とする請求項２又は６記載の伝送システム。

【請求項１０】　上記ソース装置及び上記シンク装置は、それぞれ、

共通のキーに基づいて上記第１のキーを生成する第１のハッシュ回路と、

上記共通のキーに基づいて上記第２のキーを生成する第２のハッシュ回路とを

備え、

上記情報パケットが上記シンク装置によって受信される前に、上記共通のキーが、上記シンク装置及び上記ソース装置間で伝送されることを特徴とする請求項６記載の伝送システム。

【請求項１１】　コピー保護モードを有し、情報を伝送する伝送方法において、

ソース装置が、コピー保護モードを有する情報パケットを受信するステップと、

上記ソース装置が、上記コピー保護モードに従って、暗号化モード識別子（ＥＭＩ）コードを上記情報パケットのヘッダに格納するステップと、

上記ソース装置が、上記ＥＭＩコードが第１のモードであるときに第１の暗号化構造を用いて上記情報パケットのデータを暗号化するステップと、

上記ソース装置が、上記ＥＭＩコードが第２のモードであるときに第２の暗号化構造を用いて上記情報パケットのデータを暗号化するステップと、

上記ソース装置が、上記ＥＭＩコードが第３のモードであるときに上記情報パケットのデータを暗号化しないステップと、

上記第１のモードは、上記情報パケットがシンク装置によって再生されないことを示すコピー禁止モードであり、上記第２のモードは、上記情報パケットが上記シンク装置によって１回以上再生されないことを示す１回コピー許可モードであり、上記第３のモードは、上記情報パケットが上記シンク装置よって自由に再生されることを示す無制限モードであり、上記ソース装置が、上記シンク装置に上記情報パケットを伝送するステップとを有する伝送方法。

【請求項１２】　更に、上記シンク装置が、上記情報パケットを受信して、上記ＥＭＩコードを抽出するステップと、

上記シンク装置が、上記ＥＭＩコードが上記第１のモードであるときに第１の暗号解読構造を用いて上記情報パケットのデータを暗号解読するステップと、

上記シンク装置が、上記ＥＭＩコードが上記第２のモードであるときに第２の暗号解読構造を用いて上記情報パケットのデータを暗号解読するステップと、

上記シンク装置が、上記ＥＭＩコードが上記第３のモードであるときに上記情

報パケットのデータを暗号解読しないステップとを有する請求項１１項記載の伝送方法。

【請求項１３】　更に、上記シンク装置が、上記ＥＭＩコードを上記第２のモードから上記第１のモードに変換して、新しいＥＭＩコードを上記情報パケットに格納するステップと、

上記シンク装置が、上記情報パケットを記録するステップとを有する請求項１２項記載の伝送方法。

【請求項１４】　ソース装置が、コピー保護モードを有する情報パケットを受信する上記ステップは、上記ソース装置が、エンコードされたＣＣＩ情報を有する情報パケットを変換して、上記コピー保護モードを抽出するステップを有することを特徴とする請求項１２項記載の伝送方法。

【請求項１５】　上記情報パケットは、１まとまりの音声／画像プログラムのデジタル表現であることを特徴とする請求項１２項記載の伝送方法。

【請求項１６】　上記ソース装置は放送受信装置であり、上記シンク装置はビットストリーム記録装置であることを特徴とする請求項１２項記載の伝送方法。

【発明の詳細な説明】

【０００１】

発明の分野

本発明は、伝送システム及び伝送方法を開示する。一実施の形態において、暗号化モード識別子（encryption mode indicator）を用いて情報を伝送する伝送方法及び伝送システムを開示する。本発明は、情報通信システムの分野に関する。より詳しくは、本発明は、音声／画像作品を表す情報の安全な（secure）通信モードの分野に関する。

【０００２】

関連技術

近年、デジタルインタフェースを用いて複数の音声／画像（ＡＶ）機器を接続し、ＡＶ情報（例えば、映画、歌等のＡＶ作品を表す情報）を、情報源（例えば、ビデオディスクプレーヤ又はビデオテープレコーダ）から情報表示装置（例えば、テレビジョン受像機又はモニタ受像機）又は情報シンク装置（information sink device）に伝送する技術がある。この技術の発達によって、ＡＶ機器にＩＥＥＥ１３９４シリアル通信規格が採用されている。ＩＥＥＥ１３９４シリアル通信規格において、情報は、一定のヘッダ情報及びデータセクションを有するデジタルパケットで伝送される。

【０００３】

伝送されるＡＶデジタル情報（例えば、映画を表す情報）は、通常、著作権によって保護されており、認可されていないユーザがその情報を見たり、そのＡＶ作品を不当に再生することは禁止されている。不当なコピーを防止するために、ＡＶ情報は、コピー制御情報（Copy Control Information：ＣＣＩ）ビットと呼ばれるエンコードされたコピー制御情報と共に伝送される。ＣＣＩビットは、コピー世代管理方式（Copy Generation Management System：CGMS）ビットとも呼ばれる。

【０００４】

エンコードされたＣＣＩコードは、２ビットからなり、「００」、「１０」、及び「１１」は、それぞれ「コピーの無制限許可」、「一世代コピーの許可」、

及び「コピーの禁止」を示している。「０１」ビットコードは使用されていない。特定のＡＶ情報にどのＣＣＩビットが加えられるかは、ＡＶ情報（例えばムービングピクチャエキスパートグループＭＰＥＧ、デジタルビデオＤＶ及びオーディオデータ）の種類によって規定されている。これらのＣＣＩビットは、ＡＶ情報を構成するデータパケットのデータ部中に加えられており、下流の装置によるＡＶ情報の使用を制御している。

【０００５】

データの記録毎に、記録装置はパケットのＡＶ情報に加えられているＣＣＩコードを調べ、ＣＣＩコードがコピーの禁止を示しているときには、ＡＶ情報を記録することを禁止する。ＣＣＩコードが一世代コピーを許可しているときには、ＣＣＩコードはコピー禁止モードに変えられるとともに、ＡＶ情報は１回記録媒体に記録される。すなわち、元のデータから許可されているコピー世代は制限される。

【０００６】

更に、コピー世代の制限方式を強化するために、ＣＣＩコードが暗号化されて情報のデータ部に加えられ、その情報を解読する権利は、そのコピー世代の制限方式に適合する装置のみを製造するように契約している製造者に与えられるという方法が用いられている。記録装置が、ＡＶ情報中に暗号化されているＣＣＩコードを調べるか又は変えるためには、その装置にマイクロコンピュータを搭載するか、又はその処理のための専用のハードウェアを設ける必要がある。多くの種類のＡＶ情報と適合させるためには、必要とされる暗号解読の回路は比較的複雑となり、装置のコストも増加する。

【０００７】

例えば、ビットストリーム記録（ＢＳＲ）装置のような安価な記録装置を製造するために、上述した専用のハードウェアが取り除かれた装置はＡＶ情報中のＣＣＩコードを読むことができないことが考えられる。この安価なＢＳＲ装置において、ＡＶパケット中に、コピー保護の情報を格納するための特定のフィールドを設けることが考えられている。ＦＩＧ．１は、ＩＥＥＥ１３９４規格に基づくヘッダ部１２と、パケット（ＣＩＰ）ヘッダ部１４と、データフィールド部１６

とを有する従来の情報パケットのフィールドを示している。このデータパケットはアイソクロナスパケットである。ＣＩＰヘッダ部１４には、特化されたビットストリームコピー制御情報（ＢＣＩ）フィールド２０が含まれている。ＢＣＩフィールド２０は、ＡＶ情報がＢＳＲ装置に伝送されるときに用いられるコピー保護の情報を有している。データ部１６は暗号化されたデータを有することはできるが、ＣＩＰヘッダ部１４は、通常、ＢＳＲの限られた性能に適応するように暗号化せずに伝送する。

【０００８】

このパケット１０に対して、ＢＳＲ装置はパケットヘッダ１４のＢＣＩフィールド２０を調べて、パケットがコピー禁止を示しているときは記録をせず、パケットが一世代コピー許可又はコピー無制限許可を示しているときはデータを記録することができる。許可されると、パケットの情報は、パケットヘッダ１４に格納されているＢＣＩコード２０とともに、ＢＳＲ装置によって記録される。元のパケットヘッダが一世代コピー許可を示しているときは、記録されている情報が再生されて、ＢＳＲ装置からＩＥＥＥ１３９４バスに供給された後、再生されたＢＣＩコードはコピー禁止を示す（既に１回コピーされたためである）。しかしながら、元のＢＣＩコードが無制限コピーを示しているときは、同じＢＣＩコードは格納されて伝送される。

【０００９】

ＦＩＧ．２は、上述したコピー保護が不当な装置３４によって妨害される可能性があるシステム３０を示している。ＦＩＧ．２に示すように、ソース装置３２は、ＢＳＲ装置であるシンク装置３６に情報を伝送する。妨害装置３４が、この通信路（３８ａと３８ｂ）の間に位置している。パケットが送信装置３２からシンク装置３６に伝送されている間に、パケットヘッダ１４のＢＣＩコード２０は、妨害装置３６によって妨害される。例えば、送信装置３２は、コピー禁止を示すビットコード「１１」を有するＢＣＩコード２０を送信するが、これは、送信の際に、（妨害装置３４によって）一世代コピー許可を示すビットコード「１０」に不正に変えられるか、又は、無制限コピーを示すビットコード「００」に変えられることもある。このパケットを受信すると、パケットヘッダ１４のＢＣＩ

コードは、一世代コピー又は無制限コピーを許可しているため、ＢＳＲ３６は、そのデータが本当はコピーを禁止しているという事実を通知されずに、そのパケットの情報を記録する。すなわち、コピー世代は制御されていない。

【００１０】

したがって、パケットの情報が、妨害装置に妨害されることなく、ソース装置から知的でない装置に伝送されるコピー保護システムが必要である。更に、パケットの情報が、妨害装置に妨害されることなく、ソース装置からＢＳＲ装置に伝送されるコピー保護システムが必要である。さらに、伝送の際に、コピー保護モードの情報が変えられることなく、シンク装置に対して使用可能な値を供給する方式が必要である。本発明は、このような優れた特徴を提供するものである。先に詳細に述べていない本発明のこれら及び他の利点は、ここに示す本発明の説明において明らかになる。

【００１１】

発明の開示

暗号化モード識別子（ＥＭＩ）を用いて情報を伝送する伝送方法及び伝送システムを説明する。本発明は、例えば、著作権を有する音声／画像作品の伝送のように、コピー保護情報が装置間で伝送される用途において有効である。本発明は、伝送が個々の情報パケットで行われるＩＥＥＥ１３９４シリアル通信規格において用いることができる。

【００１２】

本発明は、（例えば、音声／画像作品を示す）データが、ソース装置からシンク装置（受信局）に伝送される際に用いられる複数の保護通信モードを提供する。第１の保護モードであるＥＭＩモードＡでは、伝送される情報が、作品全体に渡ってコピーが許可されない。これは、最も高レベルのコピー禁止である。第２の保護モードであるＥＭＩモードＢでは、伝送される情報が、シンク装置によって一世代コピーのみを許可される。第３の保護モードでは、暗号化が行われず、自由なコピーが可能である。モードＡ及びモードＢのいずれの保護モードが選択されるかによって、ソース装置は伝送情報を暗号化する際に異なる暗号化処理を用いる。更に、モードＡ及びモードＢのいずれの保護モードが選択されるかによ

って、シンク装置は伝送情報を暗号解読する際に異なる暗号解読処理を用いる。すなわち、ＥＭＩコードは、（１）伝送情報のコピー保護モードと、（２）使用される暗号化処理の両方を示している。

【００１３】

本発明は、ソース装置と、パケットヘッダからコピー制御情報を抽出する能力を備えていないビットストリーム記録装置との間での伝送に特に有効である。各伝送モードによって異なる暗号化処理を行うことによって、選択される暗号解読処理は、行われた暗号化処理とは異なるため、ソース装置とシンク装置との間に位置してＥＭＩコードを変更する不当な装置は、音声／画像作品をその後再生したり記録したりすることはできない。

【００１４】

本発明の一実施の形態では、１つの暗号化処理が用いられるが、データを暗号解読するのに、２つの異なる暗号キー（キーＡ及びキーＢ）が用いられる。この実施の形態では、パケットヘッダに格納されるＥＭＩコードに対応する暗号キーを用いて、情報が暗号化される。ＥＭＩコードがモードＡからモードＢに変換されるとき、シンク装置は、キーＢを用いて伝送信号を暗号解読する。この例では、暗号化はキーＡによって行われているため、シンク装置によって得られるものは、無意味な数字である。シンク装置において再生されるものは、そのシンク装置によって記録されたとしても、全く元のＡＶ情報ではなく、無意味なものとなる。

【００１５】

発明を実施するための最良の形態

以下に示す、ソース装置とビットストリーム記録（ＢＳＲ）装置との間におけるコピー保護の情報の安全な伝送を提供するための本発明を適用した方法及び装置の詳細な説明では、本発明の十分な理解のために、多数の具体的な説明を行う。しかし、本発明は、これらの具体的な説明の範囲内に限定されるものではなく、同等な物においても実行されうるということは、当該技術分野の専門家によって認識される。他の例では、本発明の要点を不必要に曖昧にしないために、周知の方法、工程、構成要素、及び回路は、詳細に説明しないこととする。

【００１６】

本発明では、パケットがソース装置から伝送されるときに、ＡＶパケットの情報が暗号化され、使用される暗号モード又は暗号処理は、暗号化モード識別子（ＥＭＩ）コードに従って変えられる。本発明のＥＭＩコードは、コピー禁止モード、一世代コピー許可モード、無制限モードという３つの条件を表している。「一世代コピー」という用語は、元の作品は、それから多数のコピーを作ることは許可されているが、元の作品のコピー（例えば、シンク装置に送られたもの）は、１回のみコピーできるということを意味している。選択された暗号モードを示すＥＭＩ情報は、パケットヘッダに格納される。ＥＭＩ情報が受信側で傍受されると、シンク（受信）装置は、本当の暗号モードとは異なる暗号モードで暗号を解読することになるため、パケットから正しいＡＶ情報を取得することができない。一実施の形態では、暗号モードは、暗号処理及び暗号キーを有しており、レジスタの初期値を有することもできる。

【００１７】

更に、送信装置及びシンク装置が、情報のパケットに加えられているＥＭＩ情報を理解できるかどうかによって、個々の通信は、異なる暗号モードを用いるように分類され、送信装置及びシンク装置が、他方の装置を認識できるようにする。

【００１８】

ＥＭＩ保護通信モード

ＦＩＧ．３は、本発明を適用した多数の装置構成要素を含む具体的なシステム１００を示すブロック図である。システム１００は、例えば、放送チャンネル１１５を介して、デジタル番組を表すデジタルＡＶ情報を通信することができる無線送信機１１０を含んでいる。一実施の形態では、送信機１１０は、衛星放送の送信機であってもよい。他の実施の形態では、伝送線１１５は、無線ではなく、有線である。この場合、送信機１１０は、ケーブル又は有料テレビジョン放送会社の地上配備の送信機である。

【００１９】

システム１００は、また、デジタル放送受信機１２０を含んでいる。このデジ

タル放送受信機１２０は、セットトップボックス（ＳＴＢ）とも呼ばれる。ここでは、デジタル放送受信機１２０は、ソース装置１２０と呼ばれる。ソース装置１２０は、本発明を適用したＥＭＩ回路１５０を備えており、後述するように、多数のＥＭＩ通信モードをサポートする。ＥＭＩ回路１５０は、各ＥＭＩ暗号モードによって異なる暗号構造を用いる。ソース装置１２０は、知的な装置であり、コピー保護の規格に準拠した処理を行う専用の回路を備える。例えば、ソース装置１２０は、伝送線１１５を介してデジタル番組を受信し、このデジタル番組は、コピー制御情報（ＣＣＩ情報）を用いてエンコードされる。

【００２０】

ＦＩＧ．３のシステム１００は、また、シンク装置１３０を含んでおり、この具体例では、シンク装置１３０はビットストリーム記録（ＢＳＲ）装置１３０であり、シリアルインタフェース１２５を介してソース装置１２０に接続されている。シンク装置１３０は、ＢＳＲ装置として示されているが、ＦＩＧ．８に示すどの受信装置でもよい。多くの場合、シンク装置１３０は、コストを抑えるために、比較的簡易な装置であり、全てのコピー保護の規格に準拠した処理を行うのに必要な全種類の専用の回路を備えているわけではない。例えば、シンク装置１３０は、ＣＣＩコードのＡＶ情報をデコードする能力を持っていない。しかしながら、シンク装置１３０は、本発明を適用したＥＭＩ回路１６０を備えている。ＥＭＩ回路１６０は、ＥＭＩコードに従って暗号化されたＡＶ情報のパケットを暗号解読（復号）する能力を有している。シンク装置１３０は、シリアルインタフェース１２５を介してソース装置１２０からのデジタル情報を受信するために、ソース装置１２０に接続されている。デジタル情報は、ＩＥＥＥ１３９４通信規格を用い、シリアルインタフェース１２５を介して伝送される。更に、この情報は　ヘッダ部のヘッダ情報及びデータ部のＡＶ情報（例えばデータ）を有するデジタルデータパケットの状態で伝送される。

【００２１】

後述するが、ＦＩＧ．８のＥＭＩ回路１５０及び１６０は、それぞれが２つの暗号回路を備え、シリアルインタフェース１２５を介して伝送される情報が、少なくとも２つの異なる暗号構造Ａ及びＢのもとでエンコードされるようになって

いる。一実施の形態では、ＥＭＩ回路１６０は、２つの暗号回路を備えており、モードＡ又はモードＢのいずれかの暗号構造で、シリアルインタフェース１２５を介して受信した情報を（許可されれば）暗号解読できるようになっている。本発明では、ＢＣＩコードを用いるのではなく、シリアルインタフェース１２５を通るデータパケットに入っているＥＭＩコードを用いる。ＥＭＩコードは、コピー保護モードを決定するだけでなく、パケットのデータ部で用いられる暗号モードをも決定する。すなわち、シンク装置１３０中のＥＭＩ回路１６０は、ＥＭＩモードを用いて適切な暗号解読構成を選択し、シリアルインタフェース１２５を介して受信された情報を暗号解読する。もし、本発明を適用したＥＭＩコードが、シンク装置１３０とソース装置１２０との間で、（例えば、中間の妨害装置によって）改ざんされた場合、本発明を適用したＥＭＩ回路１６０は、不適切な暗号解読モードを選択してしまう。この具体例では、元の情報は、シンク装置１３０によって受信されない。

【００２２】

シリアルインタフェース１２５を介して伝送されるＡＶ情報のパケットには、３つの種類がある。これらは、コピー許可情報と、１回コピー情報と、コピー禁止情報である。本発明では、この３種類の情報コピー保護は、異なる保護レベルを有している。コピー保護が各パケットに施される状態は、ＥＭＩモードと呼ばれる。後述するように、本発明では、ＥＭＩモードは、そのＥＭＩモードが施されたＡＶ情報に適用される暗号化モードをも示している。

【００２３】

本発明を適用した暗号すなわちＥＭＩモードを以下に説明する。ＥＭＩモードＡは、パケットのデータのコピーが禁止されていることを示す際に用いられる。このＥＭＩモードＡにおいては、ＡＶ情報は再生装置（例えば、テレビジョン受像機又はモニタ受像機）においてのみ再生可能だが、ＡＶ情報が記録されることは許可されていない。ＥＭＩモードＢは、ＡＶ情報のコピー（例えば、記録）が１回のみ可能で一世代コピーが許可されていることを示す際に用いられる。このＥＭＩモードＢは、一世代コピー許可モードとも呼ばれる。ＥＭＩモードＯは、ＡＶ情報にコピー保護がなく、コピーの制限がないときに用いられる。このＥＭ

ＩモードＯは、無制限モードとも呼ばれる。説明を簡潔にするために、本発明では、ＥＭＩモードＯでは、暗号化が行われない。ＡＶ情報が、ｎ回のコピー（ｎ＞１）を許可するコピー制御状態にあるとき、それぞれのｎ回のコピーに対応するモードを定義することによって、コピー回数を増やすことができる。

【００２４】

ＥＭＩモードは、多数の周知のエンコード技術を用いて表すことができ、少なくとも２ビットを有するレジスタを用いて示すことができる。本発明の一実施の形態では、２ビットのレジスタが用いられる。表１は、各ＥＭＩモードにおける具体的な符号化の数値を示している。なお、表１において選択されている符号化の数値は一例であり、３種類の固有の数値の一集ならなんでも用いることができる。

【００２５】

【表１】

ＥＭＩモード	２ビットの数値	説明
モードＡ	１１	コピー禁止
モードＢ	１０	１回コピー
モードＯ	００	コピー無制限
保留	０１	

【００２６】

シリアルインタフェース１２５を介して受信されるＡＶ情報は、多様なプログラムを含んでいると考えられる。各プログラムは、それ固有の保護レベルを有している。この場合、コピー禁止ストリーム（コード１１）は、少なくとも１個のコピー禁止プログラムを含むストリームである。１回コピーストリーム（コード１０）は、コピー禁止プログラムを含まず、少なくとも１個の１回コピープログラムを含むストリームである。ビットストリーム記録（ＢＳＲ）装置であるシンク装置１３０（ＦＩＧ．３）の具体例においては、シンク装置１３０は、ＥＭＩモードＢ（又はＥＭＩモードＯ）において受信されるＡＶ情報のみを記録するこ

とができ、ＥＭＩモードＡにおいて受信されるＡＶ情報のみを通過させる（拒否する）ことができる。

【００２７】

ＦＩＧ．４は、（ＦＩＧ．３における）ソース装置１２０からシンク装置１３０に送信される本発明を適用した典型的な情報パケット２００を構成するフィールドを示している。一実施の形態において、ＦＩＧ．４の情報パケット２００は、ＩＥＥＥ１３９４通信規格に準拠しているため、この情報パケット２００は、ＩＥＥＥ１３９４のヘッダ部２３０を含んでいる。このヘッダ部２３０は、ｄａｔａ＿ｌｅｎｇｔｈフィールドと、ｔａｇフィールドと、ｃｈａｎｎｅｌフィールドと、ｔｃｏｄｅフィールドと、ｓｙフィールドとを含んでいる。ヘッダ部２３０は、周知のＩＥＥＥ１３９４通信規格に準拠しており、ｔａｇフィールド及びｔｃｏｄｅフィールド以外のフィールドは、この規格において定義されている。ｔａｇフィールドは、データフィールドがＣＩＰヘッダ部２４０から始めることを示している。ｔｃｏｄｅフィールドは、２個の所定の値のうちの１個の値である。データストリームは、１つの１３９４アイソクロナスチャンネルにおける情報のストリームを意味している。

【００２８】

情報パケット２００は、また、ＣＩＰヘッダ部２４０を含んでいる。本発明においては、ＣＩＰヘッダ部２４０は、一実施の形態において、２ビット分の幅を有し、表１で定義されるようなＥＭＩモードの値を有しているＥＭＩフィールド２１０を含んでいる。ＥＭＩモードの値は、データフィールド２５０におけるデータ部２２０に対応した特定の保護通信モードに相当する。後述するように、ＥＭＩフィールド２１０において示されるＥＭＩモードは、（１）選択された特定の保護通信モード（例えば、モードＡ、モードＢ又はモードＯ）及び（２）情報パケット２００において用いられる暗号化の技術の特定の種類とを示している。本発明では、情報が（ＦＩＧ．３の）ＩＥＥＥ１３９４のシリアルインタフェース１２５を介して伝送される際に、（ＥＭＩモードＡ又はＥＭＩモードＢのとき）情報パケット２００のデータ部２２０は暗号化されるが、ヘッダ部２３０及びＣＩＰヘッダ部２４０は暗号化されない。

【００２９】

ＥＭＩフィールド２１０中のＥＭＩモードは、１３９４のアイソクロナスストリームにおけるデータストリームのコピー制御の状態を示している。本発明を適用したデータストリームは、幾つかの画像及び／又は音声のプログラムからなり、それらはそれぞれ各プログラムに対応した異なるコピー制御情報を有している可能性があると考えられる。例えば、ソース装置から出力されたＭＰＥＧの伝送ストリームは、いくつかのプログラムを含んでおり、各プログラムのコピー保護は異なるレベルを有している可能性がある。ソース装置は、ストリーム中で最も規制されたプログラムに対してＥＭＩの値を割り当てる。ビットストリーム記録装置は、ＥＭＩの値に基づいて、全てのストリームを記録するか否かを決定する。ストリーム中の各プログラムを個々に処理することができ、また、各プログラムに対応したコピー制御情報を解釈することができる別の種類の記録装置を、フォーマット認識記録装置と呼ぶ。フォーマット認識記録装置は、各プログラムに対応したコピー制御情報を参照し、その動作を決定する。

【００３０】

本発明を適用したＥＭＩ回路

ＦＩＧ．５Ａは、ソース装置１２０及びシンク装置１３０を備える本発明を適用したシステム４００の具体的構成を示すブロック図である。ＦＩＧ．５Ａは、典型的なソース装置１２０のＥＭＩ回路１５０をより詳細に示している。ソース装置１２０は、ＥＭＩ回路１５０の他に（説明を明確にするためにここでは示さないが）多数の周知の回路を備える放送受信機と呼ばれるセットトップボックス（ＳＴＲ）装置であってもよい。受信回路４１０は、ＡＶ情報をデータパケットとして受信し、コピー制御情報（ＣＣＩ）の規格において必要とされる暗号化を行う。その結果は、通信インタフェース４３０を介して出力されるとともに、インタフェース４１３を介してデマルチプレクサ（ＤＥＭＵＸ）４１４にも供給される。回路４１２は、ＥＭＩモード選択回路であり、コピー保護が必要なとき、再生されたＣＣＩに応じて、コピー保護情報としてＥＭＩモードＡかＥＭＩモードＢのいずれかを選択する。コピー保護が必要でないとき、インタフェース４１３は、シリアルインタフェース１２５に直接つながり、データパケットのＥＭＩ

フィールド２１０にＥＭＩモードＯ（コード「００」）が割り当てられる。

【００３１】

コピー保護が必要であるとき、ＥＭＩモード選択回路４１２は、信号線４２６上の信号によってＤＥＭＵＸ４１４を制御する。ＥＭＩモードＡが選択されると、インタフェース４１３からのデータパケットは、暗号化部Ａ４１８に供給され、暗号化部Ａ４１８は、暗号キー４１６及び独自の第１の暗号化技術に従ってデータパケットのデータ部（例えばデータ部２２０）を暗号化する。暗号化部Ａ４１８は、また、データパケットのＥＭＩフィールド２１０中に「１１」のコード（ＥＭＩモードＡ）を挿入する。その結果は、信号線４２６によって制御されるマルチプレクサ（ＭＵＸ）４２２に供給される。ＭＵＸ４２２は、任意の出力ドライバ４２４を用い、暗号化部Ａ４１８から出力信号をシリアルインタフェース１２５に出力する。ＥＭＩモードＢが選択されていると、インタフェース４１３からのデータパケットは、暗号化部Ｂ４２０に供給され、暗号化部Ｂ４２０は、暗号キー４１６及び独自の第２の暗号化技術に従ってデータパケットのデータ部（例えばデータ部２２０）を暗号化する。暗号化部Ｂ４２０は、また、データパケットのＥＭＩフィールド２１０中に「１０」のコード（ＥＭＩモードＢ）を挿入する。その結果は、信号線４２６によって制御されているマルチプレクサ（ＭＵＸ）４２２に供給される。ＭＵＸ４２２は、任意の出力ドライバ４２４を用いて、暗号化部Ｂ４２０から出力信号をシリアルインタフェース１２５に出力する。この実施の形態では、２つの異なる暗号化部が用いられ、２つの暗号化構造を提供する共通の暗号キー４１６に基づいて暗号化が行われる。後述するように、暗号キー４１６は、ソース装置－シンク装置間の認証処理の際に確立する。

【００３２】

ＦＩＧ．５Ａのシンク装置１３０は、ＥＭＩ回路１６０の他に（説明を明確にするためにここでは示さないが）多数の周知の回路を備えている。ＦＩＧ．５Ａのシンク装置１３０中のＥＭＩ回路１６０は、解読キー４５２が暗号キー４１６と一致していることを想定して、暗号化部Ａ４１８によって行われた暗号化を解読することができる暗号解読部Ａ４４８と、解読キー４５２が正しいことを想定して、暗号化部Ｂ４２０によって行われた暗号化を解読することができる暗号解

読部Ｂ４５０とを備えている。データパケットが、シリアルインタフェース１２５を介してデマルチプレクサ回路（ＤＥＭＵＸ）４２０とＥＭＩモード抽出回路４４０によって受信される。ＥＭＩモード抽出回路４４０は、供給されたデータパケットからヘッダ情報を抽出し、ヘッダ情報からＥＭＩフィールド２１０を抽出する。抽出されたＥＭＩモードに応じて、ＥＭＩモード抽出回路４４０は、信号線４４６上の信号を制御する。ＥＭＩモードＯが抽出されると、シリアルインタフェース１２５上のデータパケットは、直接ビットストリーム記録（ＭＳＲ）媒体４５６に供給されるか、又は、何ら変更されることなしに信号線４７０に直接出力される。

【００３３】

ＥＭＩモード抽出回路４４０がＥＭＩモードＡを抽出すると、シリアルインタフェース１２５を介して伝送されてきたデータパケットは、ＤＥＭＵＸ４４２を通って暗号解読部Ａ４４８に供給され、暗号解読部Ａ４４８は、（解読キー４５２を用いて）データパケットのデータ部を暗号解読し、結果を信号線４４６によって制御されるマルチプレクサ（ＭＵＸ）４５４に供給する。ＭＵＸ４５４は、暗号解読部Ａ４４８からのデータパケットを信号線４７０にのみ出力する。シンク装置１３０がＢＳＲ装置であるとき、ＥＭＩコードＡのデータパケットを記録することは許可されないため、この場合、ＢＳＲ媒体４５６への記録は禁止される。ＥＭＩモード抽出回路４４０がＥＭＩモードＢを抽出すると、シリアルインタフェース１２５を介して伝送されてきたデータパケットは、ＤＥＭＵＸ４４２を通って暗号解読部Ｂ４５０に供給され、暗号解読部Ｂ４５０は、データパケットのデータ部を暗号解読するとともに、ＥＭＩモードをＥＭＩモードＡに変え、ＥＭＩフィールド２１０に「１１」コードを格納し、結果を信号線４４６によって制御されるＭＵＸ４５４に供給する。ＭＵＸ４５４は、暗号解読部Ｂ４５０のデータパケットを信号線４７０に出力し、ＢＳＲ媒体４５６へのデータパケットの記録を許可し、ＥＭＩモードＡとする。シンク装置１３０がＢＳＲ装置であるとき、ＥＭＩコードＢのデータパケットを記録することは１回のみ許可され、このデータパケットは、ＢＳＲ媒体４５６に記録される前にＥＭＩモードＡに変わる。この実施の形態では、２個の異なる暗号解読部が用いられ、暗号解読は、１

つの解読キー４５２に基づいている。

【００３４】

シンク装置１３０がビットストリーム記録（ＢＳＲ）装置であるとき、ＥＭＩモードＡで暗号化されたデータを記録することは許可されない。したがって、ＥＭＩモードＡのための暗号解読部Ａは、ＢＳＲ装置では動作しない。ＦＩＧ．６Ａは、暗号化部Ａを備えないビットストリーム記録（ＢＳＲ）装置１３０におけるＥＭＩ回路６６５の具体的な構成を示すブロック図である。この実施の形態では、ＥＭＩモード抽出回路４４０は、シリアルインタフェース１２５においてＥＭＩモードＡを検出すると、暗号解読部Ｂ４５０及びＢＳＲ媒体４５６を停止させる。

【００３５】

ＦＩＧ．５Ａのシステム４００は、以下に示す方法で、妨害装置がコピー保護を妨害するのを防止する。ＥＭＩモードＡのデータパケットがシリアルインタフェース１２５上でＥＭＩモードＢのデータパケットに変更されると、シンク装置１３０は、データを再生しようとする際に不適切な暗号解読部を用いてしまうことになる。再生信号は無意味な情報となってＢＳＲ媒体４５６に記録される。ＥＭＩモードＡ又はＥＭＩモードＢのデータパケットがシリアルインタフェース１２５上でＥＭＩモードＯのデータパケットに変更されると、シンク装置１３０は、暗号解読を行わず、その信号は再生されない。

【００３６】

ＦＩＧ．５Ｂは、ソース装置１２０’及びシンク装置１３０’を備える本発明を適用したシステム５００の具体的な構成を示すブロック図である。ＦＩＧ．５Ｂは、本発明の他の実施の形態における典型的なソース装置１２０’のＥＭＩ回路１５０’と、典型的なシンク装置１３０’のＥＭＩ回路１６０’とを示している。この実施の形態では、共通の暗号化部及び共通の暗号解読部が用いられているが、それらには、選択されたＥＭＩモードに応じてそれぞれ異なるキー（キーＡ、キーＢ）が供給されるため、これにより、２種類の暗号化－暗号解読の構造が実現される。

【００３７】

ＦＩＧ．５Ｂのソース装置１２０’は、ＥＭＩ回路１５０’の他に（説明を明確にするためにここでは示さないが）多数の周知の回路を備える放送受信機と呼ばれるセットトップボックス（ＳＴＲ）装置であってもよい。受信回路５１０は、ＡＶ情報をデータパケットとして受信し、コピー制御情報（ＣＣＩ）の規格において必要とされる暗号化を行う。その結果は、（ＥＭＩモード選択回路５１４に接続する）通信インタフェース５１２を介して出力されるとともに、インタフェース５１３にも供給される。回路５１４は、ＥＭＩモード選択回路であり、コピー保護が必要なとき、再生されたＣＣＩに応じて、コピー保護情報としてＥＭＩモードＡかＥＭＩモードＢのいずれかを選択する。コピー保護が必要でないとき、インタフェース５１３は、シリアルインタフェース１２５に直接つながり、データパケットのＥＭＩフィールド２１０にＥＭＩモードＯ（コード「００」）が割り当てられる。

【００３８】

コピー保護が必要であるとき、ＥＭＩモード選択回路５１４は、マルチプレクサ（ＭＵＸ）５１６の選択線を制御する。共通の暗号キー５２４は、第１のハッシュ関数を有し、第１の暗号キー（キーＡ）をその出力として生成するハッシュ回路Ａ５２０に供給される。また、共通の暗号キー５２４は、第２のハッシュ関数を有し、第２の暗号キー（キーＢ）をその出力として生成するハッシュ回路Ｂ５２２に供給される。ＥＭＩモードＡが選択されると、ＭＵＸ５１６は、キーＡを選択して、共通の暗号化部５１８に出力し、共通の暗号化部５１８は、キーＡ及び独自の共通の暗号化技術に従ってデータパケットのデータ部（例えばデータ部２２０）を暗号化する。共通の暗号化部５１８は、また、データパケットのＥＭＩフィールド２１０中に「１１」のコード（ＥＭＩモードＡ）を挿入する。その結果は、インタフェース５３０を通って任意の出力ドライバ５２６に供給され、出力ドライバ５２６は、シリアルインタフェース１２５を介してデータパケットを出力する。

【００３９】

ＥＭＩモードＢが選択されると、ＦＩＧ．５ＢのＭＵＸ５１６は、キーＢを選択して、共通の暗号化部５１８に供給し、共通の暗号化部５１８は、キーＢ及び

独自の共通の暗号化技術に従ってデータパケットのデータ部（例えばデータ部２０）を暗号化する。共通の暗号化部５１８は、また、データパケットのＥＭＩフィールド２１０中に「１０」のコード（ＥＭＩモードＢ）を挿入する。その結果は、インタフェース５３０を通って任意の出力ドライバ５２６に供給され、出力ドライバ５２６は、シリアルインタフェース１２５を介してデータパケットを出力する。この実施の形態では、２個の異なるキー（Ａ及びＢ）が用いられ、１個の共通の暗号化部５１８において用いられる暗号化処理を切り換える。後述するように、共通の暗号キー５２４は、ソース装置－シンク装置間の認証処理の際に確立する。ソース装置１２０’及びシンク装置１３０’は、隠れたチャンネルキーＫｃを共有した後、ワークキーＡ及びＢを共有する。最初に、ソース装置１２０’は、シンク装置１３０’に乱数Ｎａを送信する。ソース装置１２０’及びシンク装置１３０’は、内部のＥＭＩ回路を用いて、以下の式によってワークキー（キーＡ及びＢ）を算出する。

KeyA=HKc(Na ‖ Ca)

KeyB=HKc(Na ‖ Cb)

ここで、ＨＫｃは、チャンネルキーＫｃを用いてキー化されるハッシュ関数であり、Ｃａ及びＣｂは、定数であり、ライセンスコードである。

【００４０】

ＥＭＩ回路１５０’は、１個の暗号化部５１８しか必要としないため、有利である。２つのハッシュ回路５２０、５２２が必要であるが、この回路は、第２の暗号化部を削除することによって削除された回路よりも一般的に規模が小さい。これは、ハッシュ関数をソフトウェアで実行するときに特に当てはまる。与えられたキーに対してハッシュ関数を決定する必要があるのは１回のみであるため、ハッシュ関数はソフトウェアで実行するのが有益である。

【００４１】

ＦＩＧ．５Ｂのシンク装置１３０’は、ＥＭＩ回路１６０’の他に（説明を明確にするためにここでは示さないが）多数の周知の回路を備えている。シンク装置１３０’中のＥＭＩ回路１６０’は、正しい共通のキーが供給されていることを想定して、１個の共通の暗号化部５１８によって行われた暗号化を解読するこ

とができる１個の共通の暗号解読部５４４を備えている。データパケットは、シリアルインタフェース１２５を介してＥＭＩモード抽出回路５４０によって受信される。ＥＭＩモード抽出回路５４０は、ＥＭＩモード抽出回路４４０と同様に、受信したデータパケットからヘッダ情報を抽出し、ヘッダ情報からＥＭＩフィールド２１０を抽出する。抽出されたＥＭＩモードに応じて、ＥＭＩモード抽出回路５４０は、ＭＵＸ５４２の選択線を制御する。ＥＭＩモード抽出回路５４０によってＥＭＩモードＯが抽出されると、シリアルインタフェース１２５上のデータパケットは、直接ビットストリーム記録（ＭＳＲ）媒体５５０に供給されるか、又は、信号線５７０を介して直接出力される。

【００４２】

コピー保護モードが抽出されると、ＥＭＩモード抽出回路５４０は、マルチプレクサ（ＭＵＸ）５４２の選択線を制御する。共通の解読キー５５４は、第１の暗号キー（キーＡ）を出力として生成する第１のハッシュ関数を有するハッシュ回路Ａ５４６に供給される。また、共通の解読キー５５４は、第２の暗号キー（キーＢ）を出力として生成する、第１のハッシュ関数とは異なる第２のハッシュ関数を有するハッシュ回路Ｂ５４８に供給される。ＥＭＩモードＡがデータパケットから抽出されると、ＭＵＸ５４２は、キーＡを選択して共通の暗号解読部５４４に供給し、共通の暗号解読部５４４は、キーＡ及び独自の共通の暗号解読技術に従ってデータパケットのデータ部（例えばデータ部２２０）を暗号解読する。共通の暗号解読部５４４は、また、データパケットのＥＭＩフィールド２１０中に「１１」のコード（ＥＭＩモードＡ）を挿入する。その結果は、出力線５７０のみに出力される。シンク装置１３０’がＢＳＲ装置であるとき、ＥＭＩモードＡのデータパケットを記録することは許可されないため、この場合、ＢＳＲ媒体５５０への記録は禁止される。

【００４３】

ＥＭＩモード抽出回路５４０によってＥＭＩモードＢが抽出されるとき、ＦＩＧ．５ＢのＭＵＸ５４２は、キーＢを選択して、共通の暗号解読部５４４に供給し、共通の暗号解読部５４４は、キーＢ及び独自の共通の暗号解読技術に従ってデータパケットのデータ部（例えばデータ部２２０）を暗号解読する。共通の暗

号解読部５４４は、また、データパケットのＥＭＩフィールド２１０中に「１１」のコード（ＥＭＩモードＡ）を挿入する。この時点でＥＭＩモードＡである結果は、インタフェース５５２を介してＢＳＲ媒体５５０に供給され、任意に出力線５７０に出力される。シンク装置１３０’がＢＳＲ装置であるとき、ＥＭＩモードＢのデータパケットを記録することは１回しか許可されないため、その後、ＢＳＲ媒体５５０への記録が行われる前に、このデータパケットはＥＭＩモードＡに切り換えられる。この実施の形態では、２個の異なるキー（Ａ及びＢ）が用いられ、１個の共通の暗号解読部５４４において用いられる暗号解読処理を切り換える。後述するように、（共通の暗号キー５２４と同様に）共通の解読キー５５４は、ソース装置－シンク装置間の認証処理の際に確立する。ＥＭＩ回路１６０は、１個の暗号解読部５４４しか必要としないため、有利である。２つのハッシュ回路５４６、５４８が必要であるが、この加えられた回路は、第２の暗号解読部を削除することによって削除された回路よりも一般的に規模が小さい。与えられたキーに対してハッシュ関数を決定する必要があるのは１回のみであるため、ハッシュ関数５４６、５４８はソフトウェアで実行するのが有益である。

【００４４】

シンク装置１３０’がビットストリーム記録（ＢＳＲ）装置であるとき、ＥＭＩモードＡで暗号化されたデータを記録することは許可されない。したがって、ＥＭＩモードＡのためのハッシュ回路Ａは、ＢＳＲ装置では動作しない。ＦＩＧ．６Ｂは、ハッシュ回路Ａを備えないビットストリーム記録（ＢＳＲ）装置１３０’におけるＥＭＩ回路６７０の具体的な構成を示すブロック図である。この実施の形態では、ＥＭＩモード抽出回路５４０は、シリアルインタフェース１２５においてＥＭＩモードＡを検出すると、共通の暗号解読部５５４及びＢＳＲ媒体５５０を停止させる。

【００４５】

ＦＩＧ．５Ｂのシステム５００は、以下に示す方法で、妨害装置がコピー保護を妨害するのを防止する。ＥＭＩモードＡのデータパケットがシリアルインタフェース１２５上でＥＭＩモードＢのデータパケットに変更されると、シンク装置１３０’は、データを再生しようとする際に不適切な暗号解読キー（キーＡとキ

ーＢのいずれか）を用いてしまうことになる。再生信号は無意味な情報となってＢＳＲ媒体５５０に記録される。ＥＭＩモードＡ又はＥＭＩモードＢのデータパケットがシリアルインタフェース１２５上でＥＭＩモードＯのデータパケットに変更されると、シンク装置１３０’は、暗号解読を行わず、その信号は再生されない。

【００４６】

ＦＩＧ．７は、ＦＩＧ．５Ａのシステム４００において実行される本発明を適用した処理を示すフローチャート７００である。ステップ７１０において、シンク装置とソース装置が互いに認識できるように認証処理が行われる。この処理は、様々な所定のライセンス及びサービスキーを用いて行われる。本発明を適用したステップ７１０においては、様々な種類の周知の認証処理や安全なキー変換処理が用いられてもよい。認証処理が成功すると、特定のコードが変換され、ステップ７２０に進む。認証処理が失敗すると、ステップ７１５において、フローチャート７００は、ＡＶ情報を交換せずに、最初に戻る。

【００４７】

ＦＩＧ．７のステップ７２０において、ソース装置１２０は、特定のコードを用いて、キーを暗号解読するシンク装置１３０に暗号化されたキーを送信する。この時点で、ソース装置とシンク装置との間で、暗号キー４１６と解読キー４５２は確立されており、これらのキーは同じ値を有する。ステップ７３０において、ソース装置１２０は、（例えばＣＣＩモードのような）第１のコピー保護モードを有するデータパケットを受信し、このＣＣＩモードを（例えば、コピー禁止、１回コピー、無制限のような）ＥＭＩモードに変換する。ステップ７４０において、ＥＭＩ回路１５０は、受信したデータパケットのヘッダに適切なＥＭＩモードを挿入し、ＥＭＩモードにおける２つの使用できる暗号化構造のうちの１つを用いてデータパケットのデータ部を暗号化する。その後、このデータパケットは、インタフェース１２５を介して伝送される。

【００４８】

ＦＩＧ．７のステップ７５０において、シンク装置１３０は、ＥＭＩ回路１６０を用いて、ＥＭＩモードを抽出し、抽出されたＥＭＩモードに従ってデータパ

ケットを暗号解読する。２つの使用できる暗号化構造のうちの１つは、ＥＭＩモードに基づいて用いられる。ＥＭＩモードＢが受信されたとき、この情報はＥＭＩモードＡ（全面保護）で記録される。ＥＭＩモードＡが受信されると、一切の記録が許可されない。ステップ７６０において、更にデータパケットの処理が必要であるとき、フローチャート７００はステップ７４０に戻り、次のデータパケットを処理する。必要でなければ、フローチャート７００は最初に戻る。

【００４９】

ＦＩＧ．５Ｂの他の実施の形態の処理動作は、上述した処理と似ているが、ここでは、ＦＩＧ．５Ｂにおける異なる暗号化及び暗号解読の構造を提供するために、異なるキーが用いられる。

【００５０】

本発明を適用した装置の分類

ＦＩＧ．８は、本発明を適用した複数の異なる種類の装置を示している。また、ＦＩＧ．８に示すのは、各装置によって受信及び送信される（ＥＭＩモードによって分類される）ＡＶ情報のパケットの種類である。破線の信号線は、ＥＭＩモードＢのＡＶ情報パケットを表し、実線の信号線は、ＥＭＩモードＡのＡＶ情報パケットを表している。第１の装置の分類は、装置分類Ａである。これらの装置は、それらのパケット情報にＥＭＩコードを加えることができるとともに、ＣＣＩデータを受信することができる送信装置を含む。１つの例は、（例えば、ＣＣＩフォーマットで）衛星放送を受信し、ＩＥＥＥ１３９４のバスを介してデータを送信することができるセットトップボックス（ＳＴＢ）１２０である。ＦＩＧ．８に示すように、ＳＴＢ装置１２０は、ＥＭＩモードＡ又はＥＭＩモードＢのいずれかで暗号化されたＡＶ送信パケットを生成することができる。ＳＴＢ装置１２０は、また、無制限のＡＶ情報を送信することができる。ＳＴＢ装置１２０は、出力６２６で示すように、ＥＭＩモードＢのＡＶ情報を出力し、出力６２８で示すように、ＥＭＩモードＡのＡＶ情報を出力する。

【００５１】

第２の装置の分類は、装置分類Ｂである。これらの装置は、ＡＶ情報パケット中に存在するＥＭＩ情報に応じることができる受信又はシンク装置を含む。分類

Ｂの１つの例の装置は、フォーマット認識記録装置６３０である。このフォーマット認識記録装置６３０は、いかなるＥＭＩモードで受信したＡＶ情報パケットを適切に暗号解読し、ＩＥＥＥ１３９４規格のフォーマットを用いてＡＶ情報を記録し、ＡＶ情報に加えられたＥＭＩ情報を記録し、ＩＥＥＥ１３９４規格のフォーマットを用いて、再生されたデータを送信することができる。受信したＡＶ情報がＥＭＩモードＢであるとき、それが記録されるときにはＥＭＩモードＡに変換されて、それ以上のコピーを防止する。フォーマット認識記録装置６３０は、ＥＭＩモードＡ６３２及びＥＭＩモードＢ６３４で暗号化されたＡＶ情報のパケットを受信することができるが、ＥＭＩモードＡ６３６で暗号化されたＡＶ情報のみを送信することができる。

【００５２】

第３の装置の分類は、装置分類Ｃである。これらの装置は、（例えば、ＣＣＩモードでの）特定のコピー保護情報を完全に処理するのに必要な専用の回路を備えていないために、このコピー保護情報を完全には処理することができない受信装置を含む。分類Ｃの１つの例は、ＦＩＧ．８のビットストリーム記録（ＢＳＲ）装置１３０である。このビットストリーム記録（ＢＳＲ）装置１３０は、入力６１０を介してＥＭＩモードＢで暗号化されたＡＶ情報のみを受信し、入力６１５を介してＥＭＩモードＡで暗号化されたＡＶ情報のみを送信することができる。ＥＭＩモードＢの情報が受信されたとき、ＢＳＲ装置１３０は、抽出されたＥＭＩコードを用いてＥＭＩモードＢで暗号化された情報を暗号解読し、この情報を記録することができる。ＢＳＲ装置１３０は、また、ＡＶ情報を再生し、ＩＥＥＥ１３９４規格の元でＥＭＩモードＡのこの情報を送信することができる。

【００５３】

第４の装置の分類は、装置分類Ｄである。これらの装置は、情報パケットに加えられたＥＭＩ情報を処理することができる受信装置を含む。分類Ｄの１つの例は、デジタルテレビジョン受像機６２０である。デジタルテレビジョン受像機６２０は、ＩＥＥＥ１３９４規格の元で、入力６２２を介してＥＭＩモードＢで暗号化されたＡＶ情報及び入力部６２４を介してＥＭＩモードＡで暗号化されたＡＶ情報のみを受信することができる。デジタルテレビジョン受像機６２０は、Ｅ

ＭＩモードＡ又はＥＭＩモードＢのＡＶ情報を暗号解読し、そのＡＶ情報を再生することができる。

【００５４】

暗号化及び暗号解読モードは、ある団体が実現したい機能に従って、その団体によってライセンスが得られる。その団体が表示装置を製造するとき、ＥＭＩモードＡ及びＥＭＩモードＢの暗号解読のライセンスが必要である。その団体がＢＳＲ装置１３０を製造するとき、ＥＭＩモードＢの暗号解読及びＥＭＩモードＡの暗号化が必要である。後述するように、本発明の一実施の形態において、ＥＭＩモードＡ及びＥＭＩモードＢは、ライセンスキー及びサービスキーと結合されることが可能である。

【００５５】

本発明の一実施の形態におけるサービスの分類の例

本発明の一実施の形態においては、特定の通信サービスがサポートされる。この実施の形態では、使用するサービスの種類によって、また、装置がソース装置かシンク装置かによって、特定の秘密（例えば、キーコード）が定義される。上述した送信装置及び受信装置の分類に従って、データ伝送のサービスの分類を以下に示す。サービス１における伝送は、分類Ａ、Ｂ又はＣの送信装置と、分類Ａ、Ｂ又はＣの受信装置とを含む。サービス２における伝送は、分類Ａ、Ｂ又はＣの送信装置と、分類Ｄの受信装置とを含む。サービス３における伝送は、分類Ｄの送信装置と、分類Ａ、Ｂ又はＣの受信装置とを含む。

【００５６】

例えば、サービス１の元では、ＣＣＩのコピー保護フォーマットを認識するソース装置が、このＣＣＩのフォーマットを認識するシンク装置にＡＶ情報を送信する（例えば、ＳＴＢ→表示装置、又は、ＳＴＢ→フォーマット認識記録装置）。ソース装置とシンク装置は両方ともコピー保護を有する知的な装置である。サービス２の元では、ＣＣＩのフォーマットを認識するソース装置が、ＣＣＩのフォーマットを認識しないが本発明を適用したＥＭＩコードを認識するシンク装置にＡＶ情報を伝送する。このシンク装置は、ソース装置と同レベルのコピー保護の機能を有していない。サービス３の元では、ＣＣＩのフォーマットを認識しな

いソース装置が、ＣＣＩのフォーマットを認識するシンク装置にＡＶ情報を送信する（例えば、ＤＶＨＳ→表示装置）。

【００５７】

本発明の一実施の形態では、ＥＭＩモードＡ、Ｂ及びサービス１、２、３を用いるための秘密コード（例えば、キーコード）が、上述の符号を付けた個々の分類の装置に与えられる（例えば、ライセンスされる）。認証処理の際に安全なキーの伝送を行うために、その２個の装置によって、キーコードすなわち「秘密」が用いられる。このようにして、上述したような暗号化及び暗号解読に用いられるキーが、ソース及びシンク装置の間で安全に伝送される。

【００５８】

サービス１、２、３では、送信装置と受信装置で異なるキーコードが必要である。例えば、サービス１の送信装置のキーコードは、受信装置のキーコードとは異なる。ここで、キーコードが個々の装置に供給される方法を説明する。ＦＩＧ．９の表に示すように、本発明のこの実施の形態では、８個のキーコードが用いられる。装置の分類は、ＭＰＥＧ又はＤＶのようなデータの種類によって、更に細かくしてもよい。サービスキーとライセンスキーとを含む１組が、サービス１、２及び３にそれぞれ割り当てられる。サポートされるサービスに従って、ソース装置はサービスキーを持ち、シンク装置はライセンスキーを持つ。すなわち、サービス１、２及び３は、サービスキー又はライセンスキーによって区別される。

【００５９】

例えば、ＳＴＢ装置１２０はサービス１、２を送信するため、サービスキー１及び２を有している。ＤＶＨＳ装置１３０は、サービス２を受信し、サービス３を送信するため、ライセンスキー２及びサービスキー３を有している。各サービスは、そのサービスのグループ内でサブグループに分割されてもよい。ある装置が有するべき機能によって、暗号化モード、サービスキー及びライセンスキーのある組み合わせがその装置に与えられる。例えば、表示装置６２０の場合は、ＥＭＩモードＡ及びＥＭＩモードＢの暗号解読キーとサービス１及び３のためのライセンスキーを有している。ＳＴＢ装置１２０の場合は、ＥＭＩモードＡ及びＥ

ＭＩモードＢの暗号化キーとサービス１及び２のためのサービスキーを有している。ＤＶＨＳ（ＢＳＲ）装置１３０は、ＥＭＩモードＡの暗号化キーとサービス３のためのサービスキーを有している。

【００６０】

ＦＩＧ．９に示すように、分類Ａの装置は、サービス１及び２の送信装置のキーコードと、ＥＭＩモードＡ及びＢのキーコードを必要とし、Ｓｅｃｒｅｔ１Ｔ、Ｓｅｃｒｅｔ１Ｔ、Ｓｅｃｒｅｔ２Ｔ、Ｓｅｃｒｅｔ２Ｔ、ＳｅｃｒｅｔＡ及びＳｅｃｒｅｔＢのキーコードが提供される。同様に、分類Ｂの装置は、サービス１及び３の受信装置とサービス１の送信装置のキーコードと、ＥＭＩモードＡ及びＢのキーコードを必要とし、Ｓｅｃｒｅｔ１Ｒ、Ｓｅｃｒｅｔ１Ｒ、Ｓｅｃｒｅｔ３Ｒ、Ｓｅｃｒｅｔ３Ｒ、ＳｅｃｒｅｔＡ及びＳｅｃｒｅｔＢのキーコードが提供される。分類Ｃの装置は、サービス１及び３の受信装置のキーコードと、ＥＭＩモードＡ及びＢのキーコードを必要とし、Ｓｅｃｒｅｔ１Ｒ、Ｓｅｃｒｅｔ１Ｒ、Ｓｅｃｒｅｔ３Ｒ、Ｓｅｃｒｅｔ３Ｒ、ＳｅｃｒｅｔＡ及びＳｅｃｒｅｔＢのキーコードが提供される。分類Ｄの装置は、サービス２の受信装置とサービス３の送信装置のキーコードを必要とし、Ｓｅｃｒｅｔ２Ｒ、Ｓｅｃｒｅｔ３Ｔ、ＳｅｃｒｅｔＡ及びＳｅｃｒｅｔＢのキーコードが提供される。典型的に、送信専用にモードＡを使用することと、受信専用にモードＢを使用することが必要である。

【００６１】

本発明を適用したサービスキーを用いた動作

以下、分類Ａのソース装置から、受信装置として動作する分類Ｂのシンク装置にデータパケットを伝送する処理について説明する。データパケットは、ソース装置からシンク装置に伝送され、シンク装置によって記録される。

【００６２】

送信側のソース装置は、データキーとしてＫｓｅｅｄを生成し、データパケットを暗号化する。サービス１の送信装置及び受信装置のための秘密コードＳｅｃｒｅｔ１Ｔ及びＳｅｃｒｅｔ１Ｒを用いて、ソース装置から受信側のシンク装置にデータキーＫｓｅｅｄが安全に送信される。次に、ソース装置は、Ｋｓｅｅｄ

、ＳｅｃｒｅｔＡ及びＳｅｃｒｅｔＢを用いて、モードＡの暗号化キーＡ及びモードＢの暗号化キーＢを生成する。具体的には、次の式を用いて算出される。

KeyA=h(Kseed‖SecretA)

KeyB=h(Kseed‖SecretB)

ここで、ｈはハッシュ関数を表しており、記号ａ‖ｂは、ａとｂのビット接続を表している。

【００６３】

ソース装置は、送信されてくるデータに加えられているＣＣＩの値を読む。ＣＣＩがコピー禁止を示しているとき、データパケットは、ＣＣＩと共に、モードＡの暗号キーＡによって暗号化される。ＥＭＩモード（「１１」）がＥＭＩフィールド２１０に格納され、データパケットがＩＥＥＥ１９９４インタフェースを介して送信される。ＣＣＩが一世代コピーの許可を示しているとき、データは、ＣＣＩと共に、モードＢの暗号キーＢによって暗号化され、ＥＭＩモード（「１０」）がＥＭＩフィールド２１０に格納されてパケット化され、そのパケットがＩＥＥＥ１９９４インタフェースを介して送信される。ＣＣＩが無制限コピーを示しているとき、データパケットは、暗号化されず、パケット化される。ＥＭＩモードが「００」としてＥＭＩフィールド２１０に格納され、そのパケットが送信される。したがって、データを暗号化するのに送信装置がどのキーを用いるかは、サービスによって決まるのではなく、データに加えられているＥＭＩモードによって決まる。

【００６４】

ソース装置と同様に、シンク装置は、Ｋｓｅｅｄ、ＳｅｃｒｅｔＡ及びＳｅｃｒｅｔＢからキーＡ及びキーＢを生成する。受信されたパケットのＥＭＩが、シンク装置によって調べられ、ＥＭＩモードがモードＡを示すとき、キーＡを用いてデータが暗号解読され、ＥＭＩモードがモードＢを示すとき、キーＢを用いてデータが暗号解読される。次に、暗号解読されたデータに加えられたＥＭＩモードが調べられる。ＥＭＩモードがコピー禁止を示しているとき、データは記録されない。ＥＭＩモードが一世代コピーの許可を示しているとき、ＥＭＩモードはコピー禁止に変えられて、データと共に記録される。ＥＭＩモードが無制限コピ

ーを示しているとき、データと共に記録される。

【００６５】

次に、送信装置が分類Ａの装置であり、受信装置が分類Ｄの装置であるときの処理を説明する。上述した処理のように、ソース装置はシンク装置にＫｓｅｅｄを安全に送信する。なお、ここで用いられる秘密コードは、Ｓｅｃｒｅｔ２Ｔ及びＳｅｃｒｅｔ２Ｒである。ソース装置は、上述したように、キーＡ及びキーＢを生成し、データに加えられたＥＭＩモードに従ってデータを暗号化する。ソース装置はデータパケットに適切なＥＭＩを格納し、それを送信する。

【００６６】

シンク装置は、ソース装置と同様の方法で、キーＢを生成する。シンク装置が、ライセンスの条件により受信の際にモードＡの使用が禁止されており、キーＡを生成できない場合を想定する。シンク装置は、受信されたパケットのＥＭＩモードを調べる。ＥＭＩモードがモードＡであるとき、シンク装置はそのパケットを破棄する。ＥＭＩモードがモードＢを示しているとき、シンク装置はキーＢを用いてデータを暗号解読し、そのパケットを記録する。このとき、データがモードＢによって暗号化されたことを示す情報が、データと共に記録される。ＥＭＩモードが００を示しているとき、シンク装置はそのままデータを記録する。このとき、データが暗号化されなかったことを示す情報が、データと共に記録される。

【００６７】

本発明の好ましい実施の形態である、ソース装置とビットストリーム記録（ＢＳＲ）装置との間でコピー保護情報を安全に送信するための方法及びシステムが説明されている。本発明は具体的な実施の形態で説明されたが、本発明は、このような実施の形態に限定されると考えられるべきではなく、むしろ、以下の請求の範囲に従って考えられるべきである。

【図面の簡単な説明】

【図１】

ＦＩＧ．１は、従来技術のコピー制御情報（ＣＣＩ）のインタフェースにおける情報パケット中のフィールドの構成を示す図である。

【図２】

ＦＩＧ．２は、ソース装置とシンク装置を備え、不当な妨害装置がその間に接続されている従来技術のシステムの構成を示すブロック図である。

【図３】

ＦＩＧ．３は、ソース装置とシンク装置が接続し、情報パケットの通信を行う、本発明を適用したシステムの構成を示すブロック図である。

【図４】

ＦＩＧ．４は、本発明を適用した暗号化モード識別子（ＥＭＩ）を含む情報パケット中のフィールドを示す図である。

【図５】

ＦＩＧ．５Ａは、本発明の第１の実施の形態におけるソース装置とこれに接続したシンク装置の具体的な構成を示す回路図である。

【図６】

ＦＩＧ．５Ｂは、本発明の第２の実施の形態におけるソース装置とこれに接続したシンク装置の具体的な構成を示す回路図である。

【図７】

ＦＩＧ．６Ａは、本発明の第１の実施の形態の他の実施例におけるビットストリーム記録装置の具体的な構成を示す回路図である。

【図８】

ＦＩＧ．６Ｂは、本発明の第２の実施の形態の他の実施例におけるビットストリーム記録装置の具体的な構成を示す回路図である。

【図９】

ＦＩＧ．７は、本発明を適用したソース装置とシンク装置によって行われる処理を示すフローチャートである。

【図１０】

ＦＩＧ．８は、本発明によってサポートされる異なる種類の音声／画像装置と、これらの装置の入力及び出力信号によって用いられる様々な通信モードを示す図である。

【図１１】

ＦＩＧ．９は、本発明における動作モードを示す図である。

【図１】

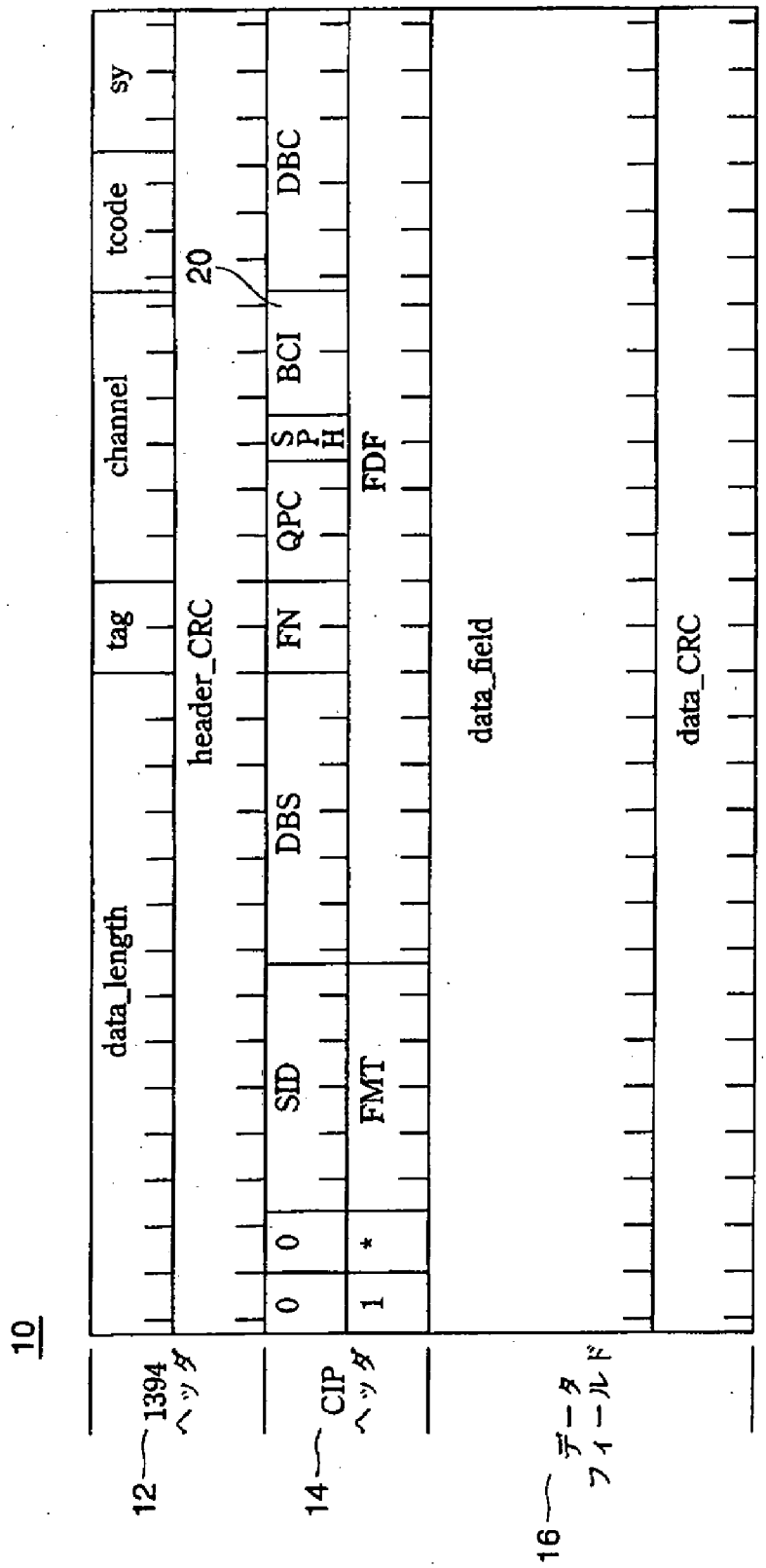
10
data_length
tag
channel
tcode
sy
header_CRC
20
DBS
FN
QPC
SPH
BCI
DBC
0
0
SID
FDF
1
*
FMT
data_field
data_CRC
12 1394 ヘッダ
14 CIP ヘッダ
16 データ フィールド
*: Form_1 (ENC)

FIGURE 1

【図２】

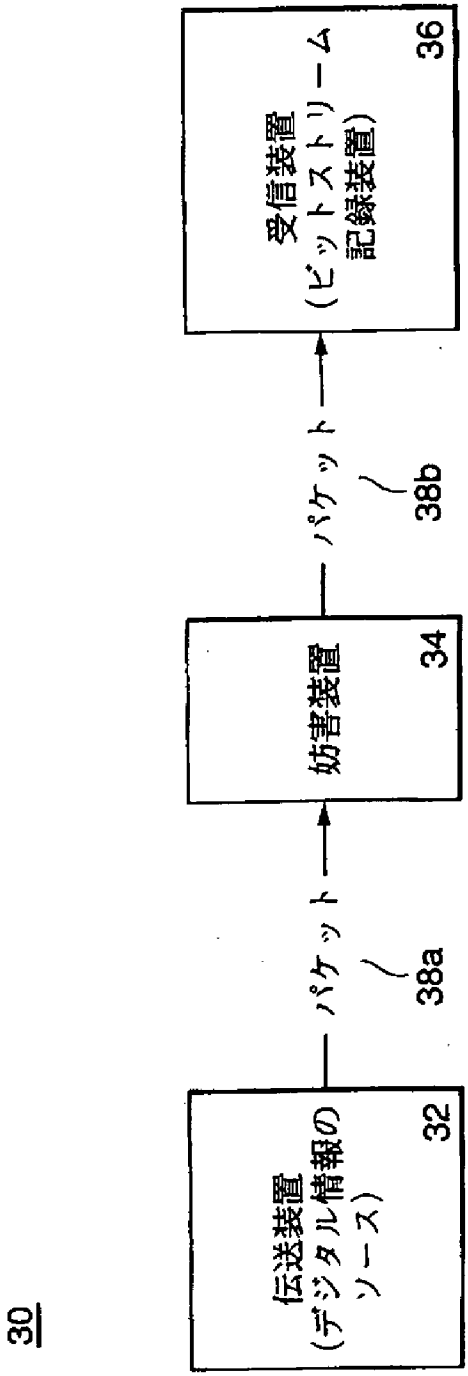

FIGURE 2
(従来技術)

【図３】

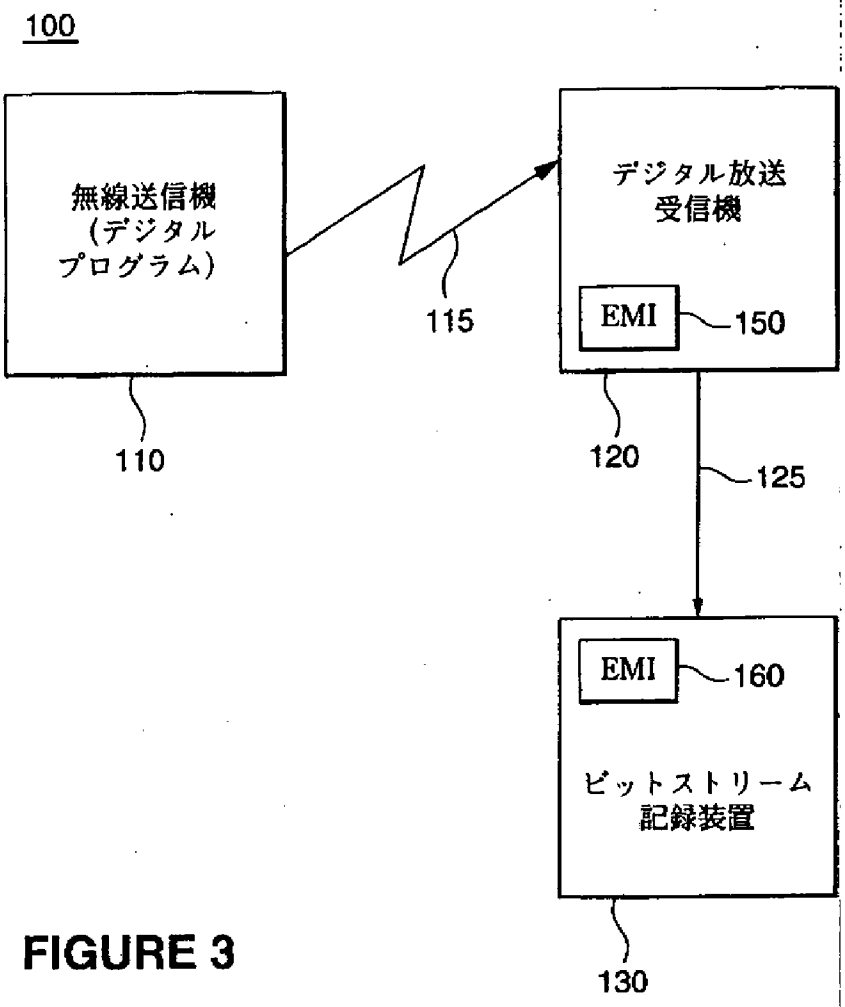
100
無線送信機
(デジタル
プログラム)
110
115
デジタル放送
受信機
EMI
150
120
125
EMI
160
ビットストリーム
記録装置
130

FIGURE 3

【図４】

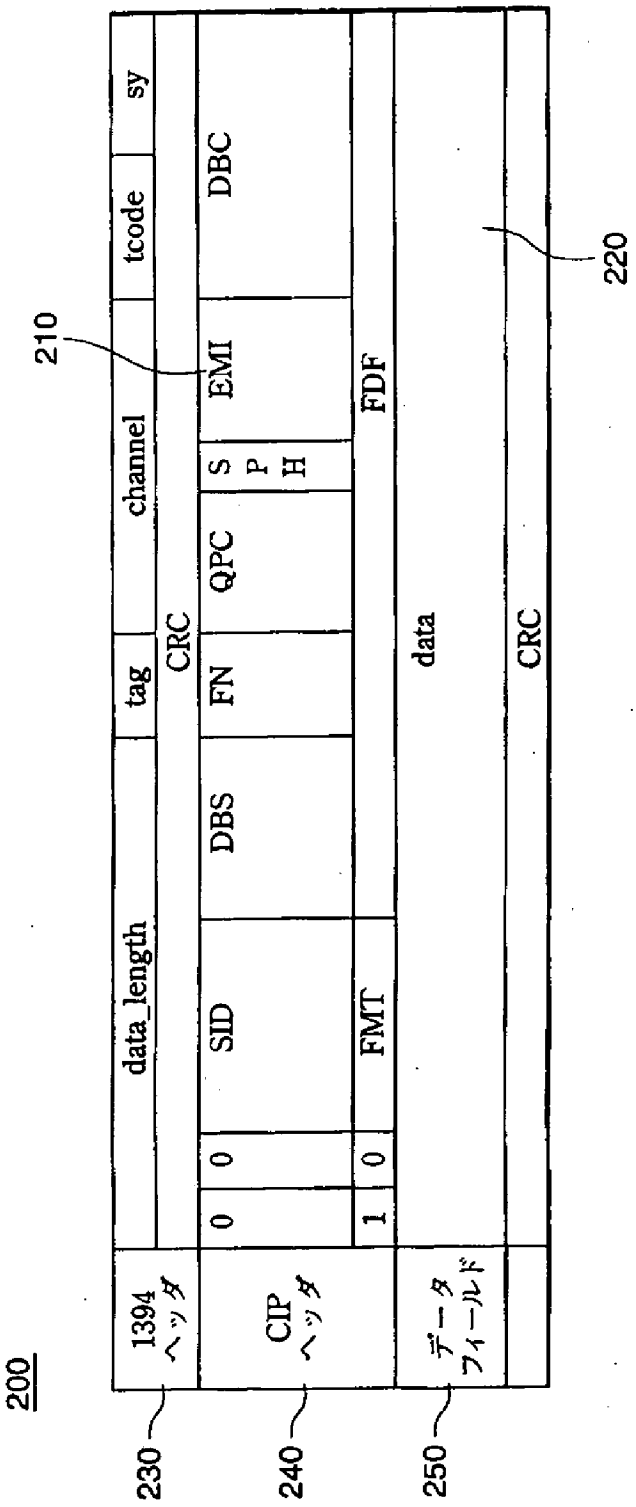
200
1394 ヘッダ
CIP ヘッダ
データ フィールド
data_length
tag
channel
tcode
sy
CRC
0
0
SID
DBS
FN
QPC
S P H
EMI
DBC
1
0
FMT
FDF
data
CRC
210
220
230
240
250

FIGURE 4

【図５】

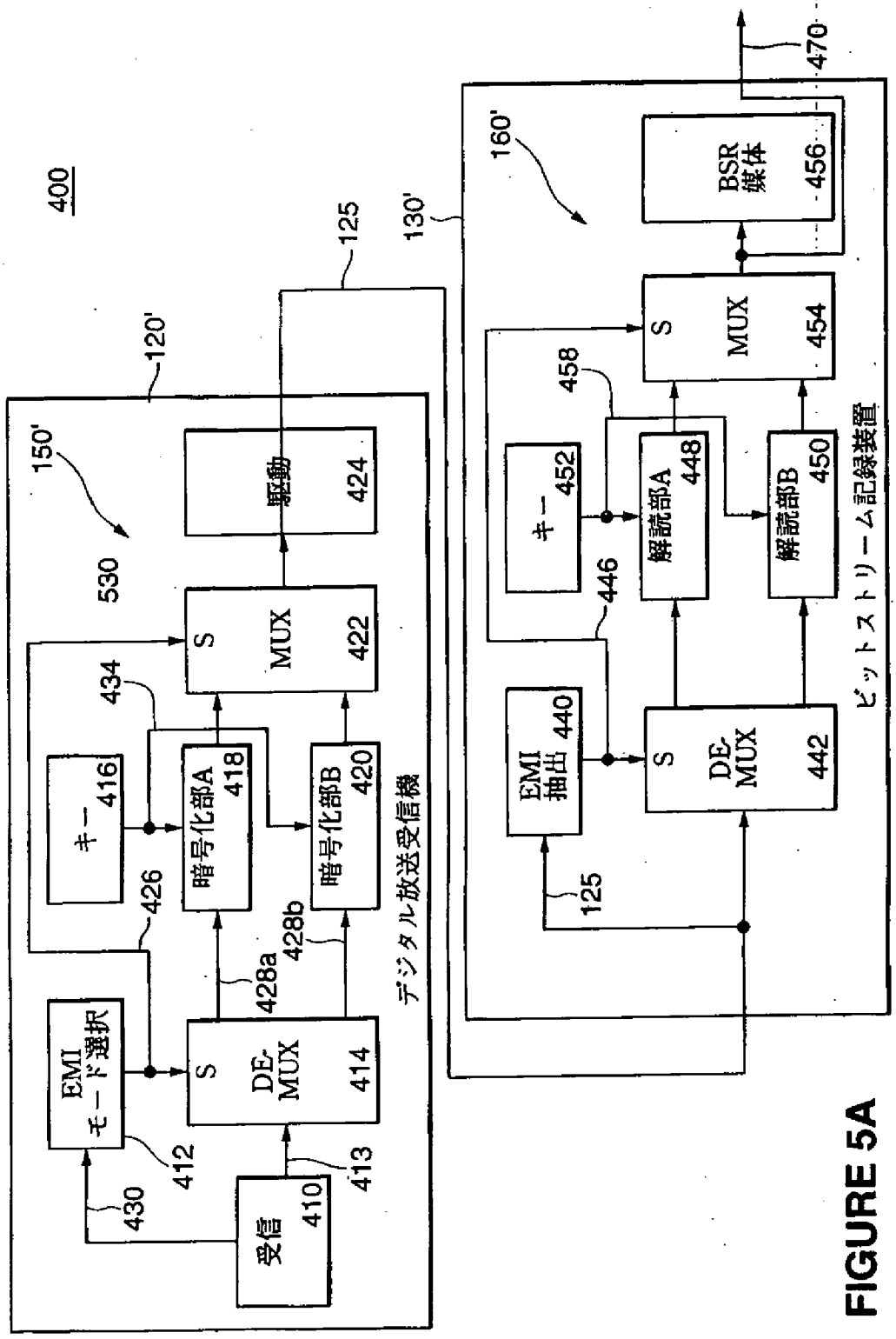
400
デジタル放送受信機
ビットストリーム記録装置
受信 410
EMI モード選択 412
DE-MUX 414
暗号化部A 418
暗号化部B 420
MUX 422
駆動 424
キー 416
EMI 抽出 440
DE-MUX 442
解読部A 448
解読部B 450
MUX 454
BSR 媒体 456
キー 452
120'
125
130'
150'
160'
413
426
428a
428b
430
434
446
458
470
530

FIGURE 5A

【図６】

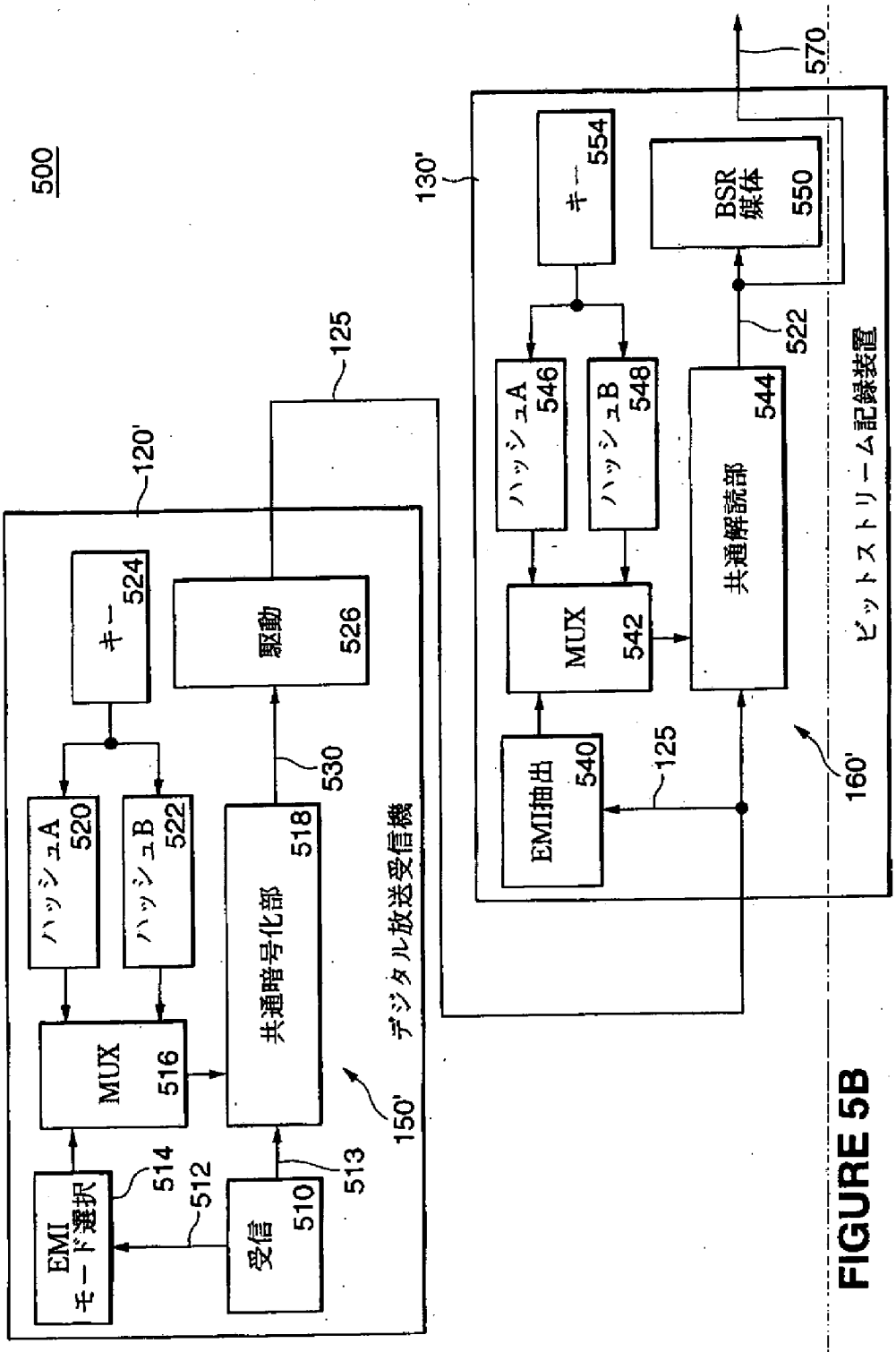
500
デジタル放送受信機
150'
ビットストリーム記録装置
160'
120'
130'
125
530
522
570
キー 524
駆動 526
ハッシュA 520
ハッシュB 522
共通暗号化部 518
MUX 516
EMI モード選択 514
受信 510
512
513
キー 554
BSR 媒体 550
ハッシュA 546
ハッシュB 548
共通解読部 544
MUX 542
EMI抽出 540

FIGURE 5B

【図７】

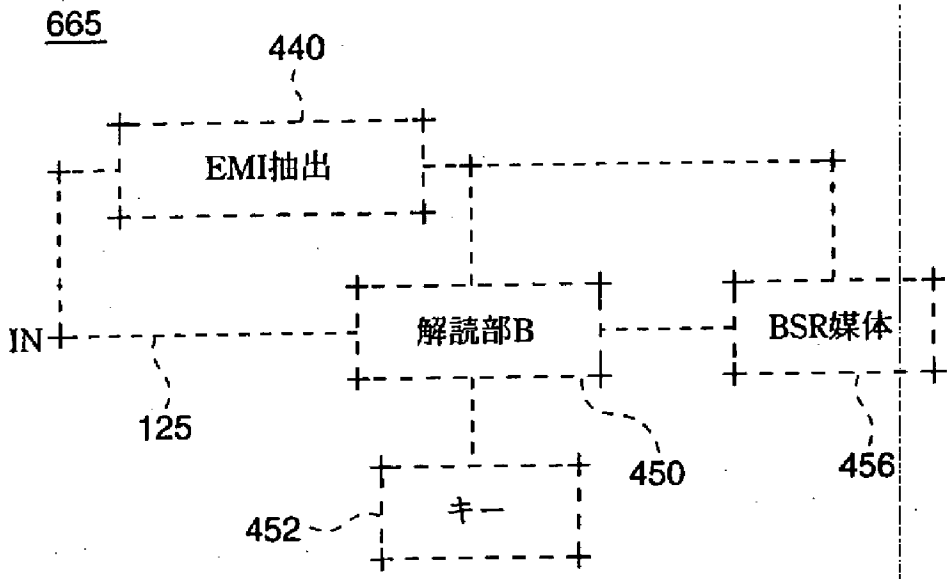

FIGURE 6A

【図８】

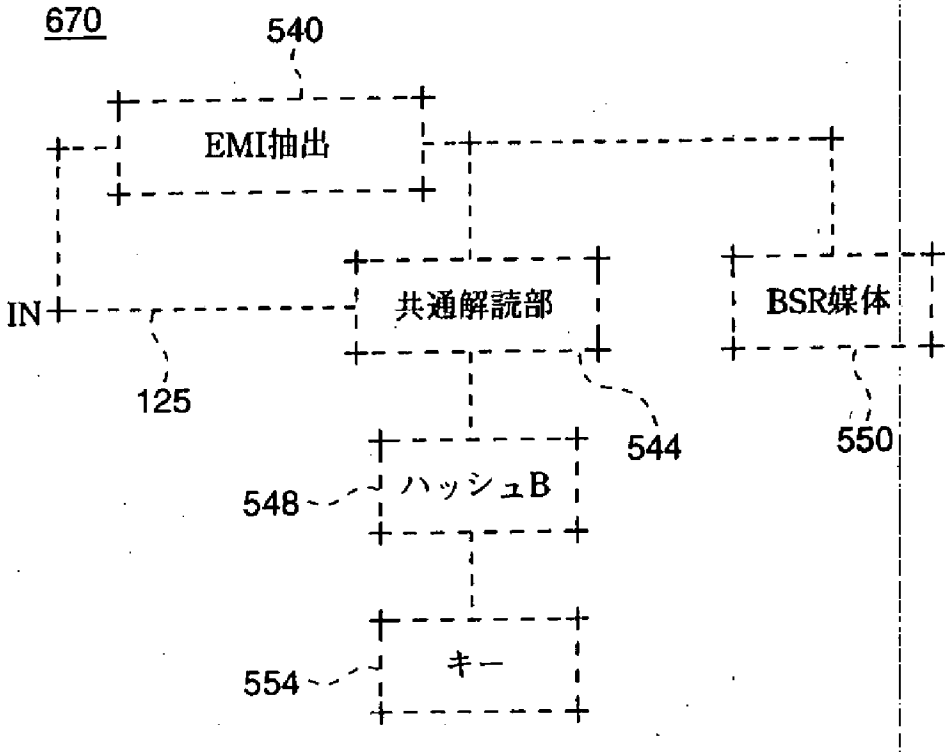

FIGURE 6B

【図９】

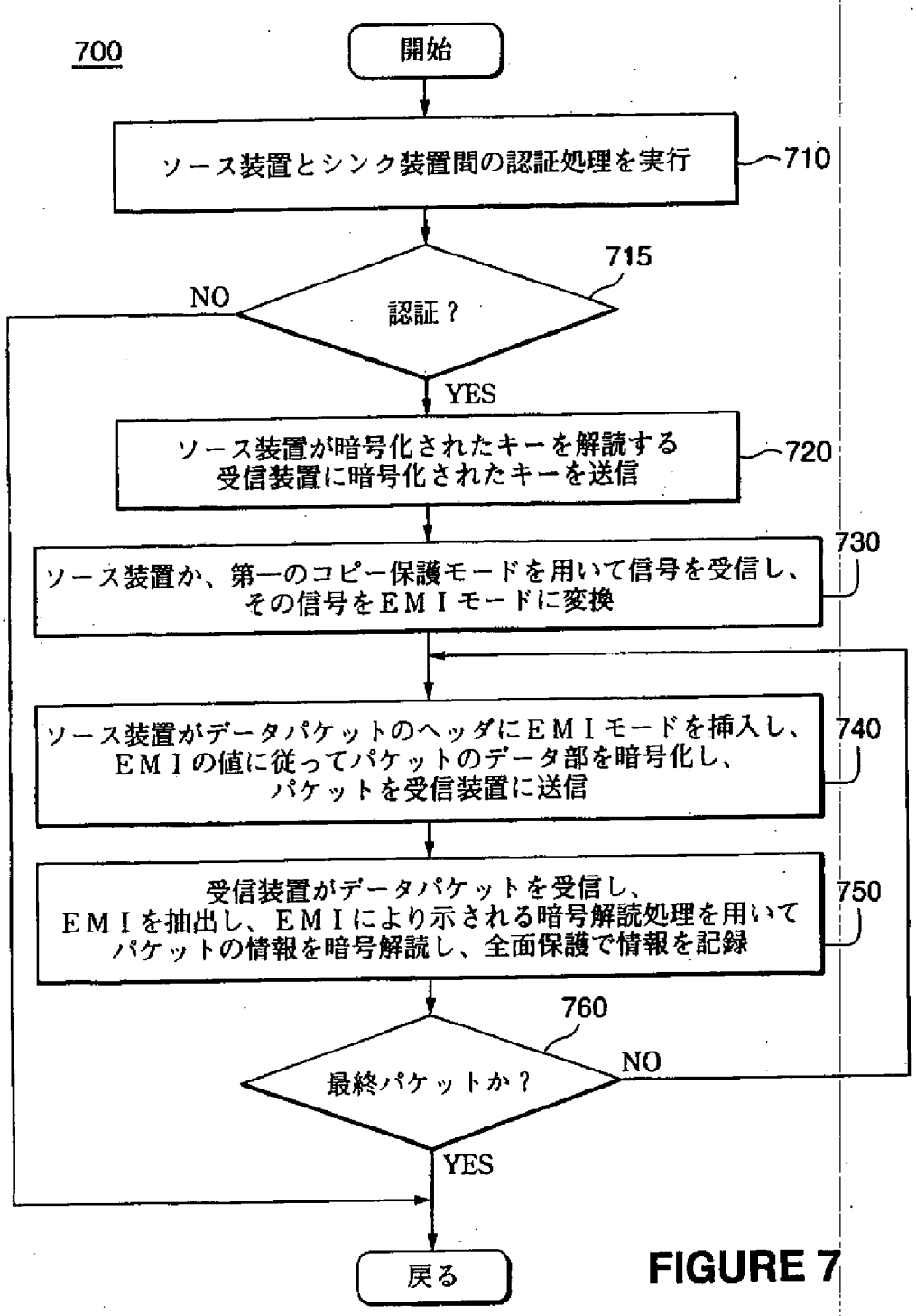
700
開始
ソース装置とシンク装置間の認証処理を実行
710
715
認証？
NO
YES
ソース装置が暗号化されたキーを解読する
受信装置に暗号化されたキーを送信
720
730
ソース装置か、第一のコピー保護モードを用いて信号を受信し、
その信号をＥＭＩモードに変換
ソース装置がデータパケットのヘッダにＥＭＩモードを挿入し、
ＥＭＩの値に従ってパケットのデータ部を暗号化し、
パケットを受信装置に送信
740
受信装置がデータパケットを受信し、
ＥＭＩを抽出し、ＥＭＩにより示される暗号解読処理を用いて
パケットの情報を暗号解読し、全面保護で情報を記録
750
760
最終パケットか？
NO
YES
戻る

FIGURE 7

【図１０】

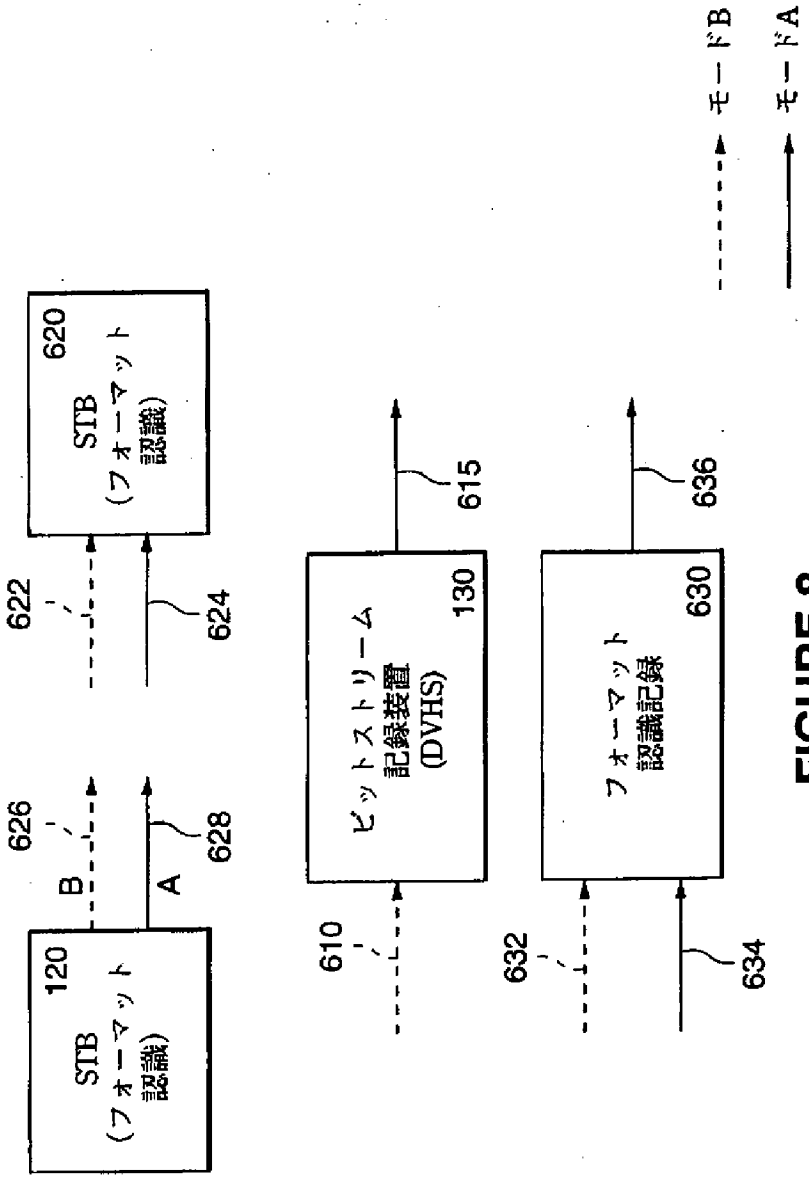
モードB
モードA
STB
(フォーマット
認識)
120
STB
(フォーマット
認識)
620
622
624
626
B
A
628
ビットストリーム
記録装置
(DVHS)
130
610
615
フォーマット
認識記録
630
632
634
636

FIGURE 8

【図１１】

300

サービス１ 310	送信 315	SECRET1T
	受信 317	SECRET1R
サービス２ 320	送信 325	SECRET2T
	受信 327	SECRET2R
サービス３ 330	送信 335	SECRET3T
	受信 337	SECRET3R
340 モードA		SECRETA
350 モードB		SECRETB

FIGURE 9

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 98/22126

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6　G11B20/00　H04N5/913

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6　G11B　H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 766 466 A (SONY CORP) 2 April 1997 see page 6, line 1 - line 44; figure 9	1,2,4-6, 9
Y	EP 0 691 787 A (SONY CORP) 10 January 1996 see the whole document	1,2,4-6, 9
A	EP 0 763 936 A (LG ELECTRONICS INC) 19 March 1997	
A	WO 97 21279 A (SOLANA TECHNOLOGY DEV CORP) 12 June 1997	
A	US 4 598 288 A (YARBROUGH CHARLES J ET AL) 1 July 1986	
A	EP 0 618 723 A (SONY CORP) 5 October 1994	

-/--

[X] Further documents are listed in the continuation of box C.　[X] Patent family members are listed in annex

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 February 1999	24/02/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Devergranne, C

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

	International Application No PCT/US 98/22126

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
E	EP 0 878 794 A (SONY CORP) 18 November 1998 see claims 1-7; figures 1-3	11-16

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int tional Application No
PCT/US 98/22126

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0766466 A	02-04-1997	JP 9098375 A	08-04-1997
		AU 6580796 A	10-04-1997
		BR 9603952 A	09-06-1998
		CA 2186418 A	30-03-1997
EP 0691787 A	10-01-1996	CN 1115150 A	17-01-1996
		JP 8077706 A	22-03-1996
		US 5796828 A	18-08-1998
EP 0763936 A	19-03-1997	CN 1150738 A	28-05-1997
		JP 9093561 A	04-04-1997
		US 5799081 A	25-08-1998
WO 9721279 A	12-06-1997	US 5719937 A	17-02-1998
		AU 1128397 A	27-06-1997
		EP 0873597 A	28-10-1998
US 4598288 A	01-07-1986	AU 536261 B	03-05-1984
		US 4305101 A	08-12-1981
		AU 6441180 A	20-05-1982
		CA 1159551 A	27-12-1983
		DE 3014309 A	06-11-1980
		FR 2454736 A	14-11-1980
		GB 2046967 A,B	19-11-1980
		JP 55141876 A	06-11-1984
EP 0618723 A	05-10-1994	JP 6339110 A	06-12-1994
		CA 2120380 A	03-10-1994
EP 0878794 A	18-11-1998	JP 10322648 A	04-12-1998
		CA 2236387 A	14-11-1998

フロントページの続き

(81)指定国　　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＣＹ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＯＡ(ＢＦ，ＢＪ，ＣＦ，ＣＧ，ＣＩ，ＣＭ，ＧＡ，ＧＮ，ＧＷ，ＭＬ，ＭＲ，ＮＥ，ＳＮ，ＴＤ，ＴＧ)，ＡＰ(ＧＨ，ＧＭ，ＫＥ，ＬＳ，ＭＷ，ＳＤ，ＳＺ，ＵＧ，ＺＷ)，ＥＡ(ＡＭ，ＡＺ，ＢＹ，ＫＧ，ＫＺ，ＭＤ，ＲＵ，ＴＪ，ＴＭ)，ＡＬ，ＡＭ，ＡＴ，ＡＵ，ＡＺ，ＢＡ，ＢＢ，ＢＧ，ＢＲ，ＢＹ，ＣＡ，ＣＨ，ＣＮ，ＣＵ，ＣＺ，ＤＥ，ＤＫ，ＥＥ，ＥＳ，ＦＩ，ＧＢ，ＧＤ，ＧＥ，ＧＨ，ＧＭ，ＨＲ，ＨＵ，ＩＤ，ＩＬ，ＩＳ，ＪＰ，ＫＥ，ＫＧ，ＫＰ，ＫＲ，ＫＺ，ＬＣ，ＬＫ，ＬＲ，ＬＳ，ＬＴ，ＬＵ，ＬＶ，ＭＤ，ＭＧ，ＭＫ，ＭＮ，ＭＷ，ＭＸ，ＮＯ，ＮＺ，ＰＬ，ＰＴ，ＲＯ，ＲＵ，ＳＤ，ＳＥ，ＳＧ，ＳＩ，ＳＫ，ＳＬ，ＴＪ，ＴＭ，ＴＲ，ＴＴ，ＵＡ，ＵＧ，ＵＺ，ＶＮ，ＹＵ，ＺＷ

(72)発明者　嶋　久登
アメリカ合衆国　カリフォルニア州　95070　サラトガ　パセオ　フロレス　12610
(72)発明者　浅野　智之
日本国神奈川県横須賀市舟倉１－15－19－202

Ｆターム(参考)　5C053 FA13 FA20 FA22 GB06 GB11 LA15
5D044 AB05 AB07 DE17 DE50 GK17 HL08

【要約の続き】
モードによって異なる暗号化処理を行うことによって、選択される暗号解読処理は、行われた暗号化処理とは異なるため、ソース装置とシンク装置との間に位置してＥＭＩコードを変更する不当な装置は、音声／画像作品をその後再生したり記録したりすることはできない。